ON THE INVERTIBILITY OF FINITE STATE MACHINES

by

Raymond R. Olson

July 23, 1970

Technical Report No. EE-703

Department of

ELECTRICAL ENGINEERING

UNIVERSITY OF NOTRE DAME, NOTRE DAME, INDIANA

ON THE INVERTIBILITY OF FINITE STATE MACHINES

by

Raymond R. Olson

July 23, 1970

Technical Report No. EE-703

Department of Electrical Engineering
University of Notre Dame
Notre Dame, Ind. 46556

This work was supported by the National Aeronautics and Space Administration (NASA Grant NGL 15-004-026) at the University of Notre Dame in liaison with the NASA Goddard Space Flight Center.

ABSTRACT

The invertibility of finite state machines is considered in detail. Necessary and sufficient conditions for the general class, as well as some important subclasses, of finite state machines to be invertible with delay L (called INV #L if L is the least delay for which an inverse exists) are given. Some structural properties of INV #L strongly connected machines with input and output sets of common order are derived. It is shown that every state on such a machine allows the same number of output sequences of length L or longer. Furthermore, it is shown that every set of final states, reachable from some known initial state with common output sequence of length L or longer, has identical cardinality.

The results of some previous research are related to this work. The concepts of information losslessness (IL) and information losslessness of finite order as established by Huffman are considered and related to invertibility. A necessary and sufficient condition for information losslessness in the case of strongly connected machines with equal order input and output sets is given.

A new type of state equivalence is presented, viz, output equivalence. It is shown that the output equivalence relation has some particularly interesting consequences in the cases of INV #L and IL machines. A state reduction of INV #L machines based on output equivalence preserves invertibility, although not necessarily inverse delay. Although state reduced IL machines do not, in

general, retain the IL property, it is shown that losslessness is preserved for the class of strongly connected machines. Several other structure preserving properties inherent in the state reduction of output equivalent states are demonstrated.

Invertibility and losslessness of the class of finite input memory machines is considered. The implications of INV #L and IL characteristics on the output function which defines output response are investigated. Sufficient conditions for output functions of non-degenerate finite input memory machines to yield INV #L and IL behavior are given.

Finite output memory machines and properties related to invertibility are examined. It is concluded that a non-degenerate finite output memory machine is invertible with zero delay or is not invertible with any delay.

A particular problem concerning the invertibility of linear finite state machines is defined and solved. The result is a necessary and sufficient condition for the existence of a feedforward inverse for a general linear finite state machine, thereby extending an earlier result of Massey and Sain. A procedure for the construction of feedforward inverses with minimal delay for linear finite state machines is also given.

Upper bounds on inverse delay for an N state machine are investigated. It is shown for a certain restricted class of binary finite state machines that the upper bound on inverse delay grows only linearly with N. By construction, it is also shown that there exists an N state, INV #L machine with $L = N(N-1)/2$ for every N. The construction, however, requires a very large output set for large values of N.

ACKNOWLEDGEMENTS

The help and encouragement received from my advisor Professor James L. Massey is gratefully acknowledged and deeply appreciated. Professor Massey's patient and inspirational guidance through a very long and trying period of graduate research has been of inestimable value. I would like to express appreciation also to my readers Professors Richard Jeffrey Leake, Ruey-Wen Liu and Michael K. Sain and to Professor Celso de Renna e Souza for valuable discussions.

The financial support received during the early portions of this research from the National Aeronautics and Space Administration (NASA Grant NGL 15-004-026) in liaison with the Goddard Space Flight Center is gratefully acknowledged. Continuing financial support received while in the employ of the Bendix Corporation under a Doctoral Work/Study Program is likewise acknowledged.

Special thanks are due to Mrs. Wilma Milburn of the Bendix Aerospace Systems Division for an excellent performance in the very tedious task of typing the final version of this manuscript.

TABLE OF CONTENTS

GLOSSARY

FSM		Finite state machine
S		State set
X	:	Input set
Y	:	Output set
δ	:	Next state map (also final state map)
λ	:	Output map (also output sequence map)
M	:	An FSM
M'	:	An inverse FSM
X^n	:	Set of length n input sequences
Y^n	:	Set of length n output sequences
x^n	:	A length n input sequence
y^n	:	A length n output sequence
Λ	:	The empty tape
N	:	State set order
$Y^n(s_i)$	:	Length n output sequence set (page 13)
$S_i(y^n)$	:	Initial state set (page 13)
$X^n(s_i, y^n)$	:	Length n input sequence set (page 13)
$S_f(s_i, y^n)$	:	Final state set (page 13)
$F^n(s_i)$	:	Length n output sequence - final state pair set (page 13)
ϕ	:	Empty set
L	:	Inverse delay
INV #L	:	Invertible with least delay L

IL	:	Information losslessness
ILF	:	Information losslessness of finite order
O_n	:	Output n-equivalence relation
π_n	:	State set partition generated by O_n
OMR	:	Output minimal representation
FIM	:	Finite input memory
FOM	:	Finite output memory
f	:	Output function
μ	:	input or output memory
LSC	:	Linear sequential circuit
G (D), H (D):		Transfer function matrices
$\underline{I}$ (D)	:	Transformed input vector
$\underline{T}$ (D)	:	Transformed output vector
A, B, C, E	:	LSC structural matrices
gcd	:	greatest common divisor
lcm	:	least common multiple

CHAPTER I

INTRODUCTION AND SOME PRELIMINARY RESULTS

There are, in many fields of engineering, a number of physical systems which can be synthesized or analyzed as finite state machines. These systems are characterized by finite input alphabets, finite output alphabets and a finite set of states or conditions which the system may assume. In addition, the behavior and response of these devices are specified by two relations; one which defines the state behavior and one which specifies the output response. Finite state machines may serve as models of digital computers, digital communication systems, numerical process controllers and other important physical systems. Hence, the study of finite state machines is not simply of academic interest, but has significant engineering application.

In the study of the behavior of physical systems certain properties and characteristics are of paramount importance. Among these properties are stability, controllability, observability and invertibility. It is the last of these characteristics which is to be considered in detail here.

Let us formally define the machine model which will be considered in our work.

Definition 1.1: A finite state machine (FSM), M, is a five-tuple, $M = <S, X, Y, \delta, \lambda>$, where S, X and Y are finite state, input and output sets respectively and δ and λ are mappings such that:

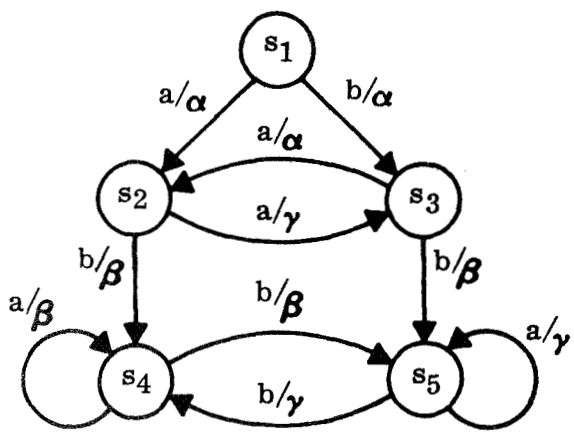
$\delta : S \times X \longrightarrow S$ and $\lambda : S \times X \longrightarrow Y$

or such that from a time viewpoint:

$\delta(s(t), x(t)) = s(t+1)$ and $\lambda(s(t), x(t)) = y(t)$ for $t = 0, 1, 2, \cdots$.

We will also refer to FSM's as sequential machines or simply as machines. No confusion should result since only FSM's will be considered in this work.

Systems such as described by Definition 1.1 may be represented by several techniques. Two of these techniques are the state diagram and the state transition table. Examples of both sequential machine representations are given in Figure 1.1.



(a) STATE TRANSITION DIAGRAM

S \ X	a	b
s_1	s_2 / α	s_3 / α
s_2	s_3 / γ	s_4 / β
s_3	s_2 / α	s_5 / β
s_4	s_4 / β	s_5 / β
s_5	s_5 / γ	s_4 / γ

(b) STATE TRANSITION TABLE

FIGURE 1.1 - TWO REPRESENTATIONS OF A FINITE STATE MACHINE, M

In the example of Figure 1.1 we have

$$S = \{ s_1, s_2, s_3, s_4, s_5 \}$$
$$X = \{ a, b \}$$
$$Y = \{ \alpha, \beta, \gamma \}$$

and the orders of the state, input and output sets are five, two and three respectively.

It is convenient to extend the definitions of input and output sets. Let X^k be the finite set of all length k sequences of elements of X. Then define X^* from

$$X^* = X^0 \cup X^1 \cup X^2 \cup \cdots\cdots = \bigcup_{i=0}^{\infty} X^i$$

where X^0 is the set containing only the sequence of length zero, i.e., only the empty tape, Λ. Similarly let Y^k be the finite set of all length k sequences of elements of Y and define

$$Y^* = Y^0 \cup Y^1 \cup Y^2 \cup \cdots\cdots = \bigcup_{i=0}^{\infty} Y^i \ .$$

Further let us extend the output and next state mappings in a corresponding way. Let λ^* be a sequence mapping such that, for any $n \geq 0$, $\lambda^*(s_i, x^n) = y^n$, $x^n \in X^n$, $y^n \in Y^n$ where y^n is the length n sequence of output letters produced from state s_i by the input sequence x^n. Let δ^* be a state mapping such that $\delta^*(s_i, x^n) = s_f$ where s_f is the final state reached from the initial state s_i by the input sequence x^n. In the work which follows the '*' symbol will be omitted in both output and state mappings since the superscript n applied to the input sequence x^n in the mappings, $\lambda(s_i, x^n)$ and $\delta(s_i, x^n)$ adequately identifies the output sequence and final state. For example in the sequential machine of Figure 1.1 if $x^6 = x_1 x_2 x_3 x_4 x_5 x_6$ = babbba, then $\lambda(s_1, x^6) = \alpha\alpha\beta\beta\gamma\beta$ and $\delta(s_1, x^6) = s_4$.

Let us now define an inverse finite state machine.

Definition 1.2: An FSM $M' = \langle S', X', Y', \delta', \lambda' \rangle$ is a delay L inverse with respect to state $s_0 \in S$ for an FSM $M = \langle S, X, Y, \delta, \lambda \rangle$ if $X' \supseteq Y$ and $Y' \supseteq X$

and if there exists $s_0' \in S'$ such that for every $n \geq 0$, for every $x^n \in X^n$ and for every $u^L \in X^L$ we have

$$\lambda'(s_0', \lambda(s_0, x^n u^L)) = \alpha^L x^n$$

for some arbitrary $\alpha^L \in Y'^L$.

We observe that, if M has a delay L inverse with respect to some state, then this clearly implies that M has a delay L+i inverse with respect to that state for every $i \geq 0$. We observe also that Definition 1.2 considers an inverse in terms of a particular initial state. The existence of an inverse with respect to one state does not guarantee that an inverse exists with respect to every state in S. If, however, for any two states, s_i and s_j, we define s_i to be reachable from s_j if there exists x^n for some $n \geq 0$ such that $\delta(s_j, x^n) = s_i$, then we have the following result.

Theorem 1.1: If an FSM, M, has a delay L inverse with respect to s_0, then M has a delay L inverse with respect to every state reachable from s_0.

Proof: Let $M' = \langle S', X', Y', \delta', \lambda' \rangle$ be a delay L inverse for $M = \langle S, X, Y, \delta, \lambda \rangle$ with respect to s_0. Let s_i be any state reachable from s_0. It follows that there exists $a^n \in X^n$ for some integer, n, such that $\delta(s_0, a^n) = s_i$. Let x^m be any length m input sequence. By Definition 1.2, there exists $s_0' \in S'$ such that

$\lambda'(s_0', \lambda(s_0, a^n x^m u^L)) = \alpha^L a^n x^m$ for some $\alpha^L \in Y'^L$ and for every $u^L \in x^L$. Let $s_i' = \delta'(s_0', \lambda(s_0, a^n))$. It follows that

$\lambda'(s_i', \lambda(s_i, x^m u^L)) = \beta^L x^m$ where β^L is the sequence containing the last L letters of $\alpha^L a^n$. Since x^m and u^L may be selected arbitrarily, it is concluded that M' is a delay L inverse for M with respect to state s_i.

We turn now to the problems of testing sequential machines for inverse existence, of determining inverse delay and of constructing an inverse when it exists. Our next result provides a necessary and sufficient condition for the existence for a delay L inverse and contains an implicit procedure for inverse construction. The construction procedure employed is similar to one given by Even[1] but is more general in that it is applicable to the general class of all machines conforming to Definition 1.1. Certain modifications of Even's procedure are necessary in the case of machines for which the next state map, δ, is not onto.

Theorem 1.2: An FSM M has a delay L inverse with respect to $s_0 \in S$ if and only if for every x^n and $u^n \in X^n$; $n = 1, 2, 3, \cdots\cdots$; $x^n \neq u^n \Rightarrow$ $\lambda(s_0, x^n v^L) \neq \lambda(s_0, u^n w^L)$ for every v^L and $w^L \in X^L$.

Proof: Let us first consider the "only if" portion of the theorem. Suppose that a machine M' is a delay L inverse for machine M with respect to state s_0. Suppose further that there exists $a^n \neq b^n \in X^n$ and c^L and $d^L \in X^L$ such that $\lambda(s_0, a^n c^L) = \lambda(s_0, b^n d^L)$. By Definition 1.2 there exists $s_0' \in S'$ such that $\lambda'(s_0', \lambda(s_0, a^n c^L)) = \alpha^L a^n$ and $\lambda'(s_0', \lambda(s_0, b^n d^L)) = \beta^L b^n$ for some α^L and $\beta^L \in Y'^L$. But by the assumption that $\lambda(s_0, a^n c^L) = \lambda(s_0, b^n d^L)$ it follows that $\alpha^L a^n = \beta^L b^n$ which is possible only if $a^n = b^n$. Hence, by contradiction, necessity is shown.

[1]S. Even, "On Information Lossless Automata of Finite Order", IEEE Transactions on Electronic Computers, Vol. EC-14, August 1965, pp 561-569.

Let us now consider the sufficiency of the condition

$$x^n \neq u^n \Rightarrow \lambda(s_0, x^n v^L) \neq \lambda(s_0, u^n w^L)$$

for the existence of a delay L inverse with respect to s_0. To prove sufficiency we assume that the condition holds and construct an inverse for M.

Let $M' = \langle S', X', Y', \delta', \lambda' \rangle$ be defined by

$$X' = Y$$

$$Y' = X$$

$$S' = \left\{ \bigcup_{i=0}^{L-1} \left\{ \left[s_0, y^i \right] : \text{ There exists } x^i \text{ such that } \lambda(s_0, x^i) = y^i \right\} \right\} \bigcup \left\{ \left[s_i, y^L \right] : \begin{array}{l} s_i \text{ reachable from } s_0 \text{ and} \\ \text{there exists } x^L \text{ such that } \lambda(s_i, x^L) = y^L \end{array} \right\} .$$

For every $\left[s_0, y^i \right] \in S'$; $0 \leq i \leq L-1$; if $\left[s_0, y^i z \right] \in S$, define δ' and λ' by

$$\delta'(\left[s_0, y^i \right], z) = \left[s_0, y^i z \right]$$

$$\lambda'(\left[s_0, y^i \right], z) = \text{an arbitrary letter from } Y'.$$

For every $\left[s_i, \alpha \beta^{L-1} \right] \in S'$ and for every z such that there exists a b^L such that $\lambda(s_i, \text{ a } b^L) = \alpha \beta^{L-1} z$ define δ' and λ' from

$$\delta'(\left[s_i, \alpha \beta^{L-1} \right], z) = \left[\delta(s_i, a), \beta^{L-1} z \right]$$

$$\lambda'(\left[s_i, \alpha \beta^{L-1} \right], z = a .$$

Since s_i is reachable from s_0 by some input sequence c^m for some m it is clear from our assumption

$$\lambda(s_0, x^n v^L) = \lambda(s_0, u^n w^L) \Rightarrow x^n = v^n$$

for all integers n, that $\lambda(s_0, c^m a b^L)$ uniquely defines the input sequence $c^m a$ and hence, the input letter a. Therefore, the mappings δ' and λ' are well defined in all cases considered. In all other cases let the next states and output letters be specified arbitrarily.

We claim that M' is a delay L inverse for M with respect to state s_0. To verify this assertion consider the result of application of any input sequence, say, x (0) x (1) x (2) ····· to M in state s (0) = s_0. Let $\lambda(s_0, x(0)\ x(1)\ x(2)\ \cdots\cdots) = y(0)\ y(1)\ y(2)\ \cdots\cdots$ be applied as an input sequence to M' in state $s'(0) = s_0' = [s_0, y^0]$, where $y^0 = \Lambda$ is the empty tape. By the construction of M' we have

$$s'(L-1) = [s_0, y(0)\ y(1)\ \cdots\cdots\ y(L-1)] .$$

Moreover, by construction we have

$$s'(L) = [\delta(s_0, x(0)), y(1)\ y(2)\ \cdots\ y(L)]$$

and $$y'(L) = x(0) .$$

Again by construction we may write

$$s'(L+1) = [\delta(s(1), x(1)), y(2)\ y(3)\ \cdots\cdots\ y(L+1)]$$

and $$y'(L+1) = x(1) .$$

By induction, it follows that for all $t \geq L$

$$s'(t) = [s(t-L+1), y(t-L+1)\ y(t-L+2)\ \cdots\cdots\ y(t)]$$

and $$y'(t) = x(t-L) .$$

Therefore, M' is a delay L inverse for M with respect to state s_0 and the condition of the theorem is sufficient for delay L inverse existence.

The constructive proof of Theorem 1.2 provides a procedure for inverse construction. To illustrate the application of Theorem 1.2 in the construction of inverses, consider the FSM M defined in Figure 1.1. It can be shown (e.g., by Theorem 1.3, to follow) that the machine of Figure 1.1 has a delay two inverse with respect to state s_1. Following the steps of the constructive proof of Theorem 1.2 for L = 2 we define such an inverse as in Figure 1.2.

	α	β	γ
$[s_1, \Lambda]$	$[s_1, \alpha]$ / Δ	Δ / Δ	Δ / Δ
$[s_1, \alpha]$	$[s_1, \alpha\alpha]$ / Δ	$[s_1, \alpha\beta]$ / Δ	$[s_1, \alpha\gamma]$ / Δ
$[s_1, \alpha\ \alpha]$	Δ / Δ	$[s_3, \alpha\beta]$ / b	$[s_3, \alpha\gamma]$ / b
$[s_1, \alpha\ \beta]$	Δ / Δ	$[s_2, \beta\beta]$ / a	$[s_3, \beta\gamma]$ / b
$[s_1, \alpha\ \gamma]$	$[s_2, \gamma\alpha]$	$[s_2, \gamma\beta]$ / a	Δ / Δ
$[s_2, \beta\ \beta]$	Δ / Δ	$[s_4, \beta\beta]$ / b	$[s_4, \beta\gamma]$ / b
$[s_2, \gamma\ \alpha]$	Δ / Δ	$[s_3, \alpha\beta]$ / a	$[s_3, \alpha\gamma]$ / a
$[s_2, \gamma\ \beta]$	Δ / Δ	Δ / Δ	$[s_3, \beta\gamma]$ / a
$[s_3, \alpha\ \beta]$	Δ / Δ	$[s_2, \beta\beta]$ / a	Δ / Δ
$[s_3, \alpha\ \gamma]$	$[s_2, \gamma\alpha]$ / a	$[s_2, \gamma\beta]$ / a	Δ / Δ
$[s_3, \beta\ \gamma]$	Δ / Δ	$[s_5, \gamma\beta]$ / b	$[s_5, \gamma\gamma]$ / b
$[s_4, \beta\ \beta]$	Δ / Δ	$[s_4, \beta\beta]$ / a	$[s_4, \beta\gamma]$ / a
$[s_4, \beta\ \gamma]$	Δ / Δ	$[s_5, \gamma\beta]$ / b	$[s_5, \gamma\gamma]$ / b
$[s_5, \gamma\ \beta]$	Δ / Δ	$[s_4, \beta\beta]$ / b	$[s_4, \beta\gamma]$ / b
$[s_5, \gamma\ \gamma]$	Δ / Δ	$[s_5, \gamma\beta]$ / a	$[s_5, \gamma\gamma]$ / a

NOTE: The symbol, Δ, indicates a "don't care" entry.

FIGURE 1.2 - M', A DELAY TWO INVERSE FOR M WITH RESPECT TO STATE s_1

The inverse machine M' should be initialized to state $[s_1, \Lambda]$ in order to properly recover the input letters of M when M is initialized to state s_1.

We note that an inverse constructed according to the procedure of Theorem 1.2 will, in general, not be minimal. Based on the construction it is possible to state an upper bound on the number of states in the minimal inverse. The maximum number of states in such an inverse follows from the definition of M' and is given by

$$
\begin{aligned}
(\#S')_{MAX} = \text{MAX}\Big[\#\bigcup_{j=0}^{L-1}\Big\{\big[s_0, y^j\big] : &\text{ there exists } x^j \text{ such that} \\
&\lambda(s_0, x^j) = y^j\Big\}\Big] \\
+ \text{MAX}\Big[\#\Big\{\big[s_i, y^L\big] : &\ s_i \text{ reachable from } s_0 \text{ and} \\
&\text{such that there exists } x^L \text{ such that} \\
&\lambda(s_i, x^L) = y^L\Big\}\Big] \\
= 1 + (\#Y) + (\#Y)^2 + \cdots\cdots + (\#Y)^{L-1} &+ (\#S)\cdot(\#Y)^L \\
= \frac{(\#Y)^L - 1}{(\#Y)-1} &+ (\#S)\cdot(\#Y)^L \ .
\end{aligned}
$$

Where #S and #Y indicate the number of states in the state set and the number of letters in the output set respectively.

An interesting characteristic of the inverse machine M' of Figure 1.2 is that, if the "don't care" entries are removed and the next state and output mappings are completely specified, M' does not have an inverse with respect to any state. This may be verified by any of several methods to be presented in later sections and is concluded as a result of Theorem 1.5 to follow. It is noted, however, that with any assignment of "don't care" entries M' remains

a delay L inverse for M with respect to state s_1. Therefore, it is not in general true that every inverse machine itself has an inverse.

Incompletely specified machines will not be considered further in this work. The introduction of "don't care" or unspecified conditions complicates the study of inverses and results in a situation in which inverses may exist for certain next state and/or output assignments, but not for others. Hence, only completely specified machines will be treated in what follows.

Of course M' is not the only inverse which may be constructed for the machine M of Figure 1.1. To illustrate the existence of two non-equivalent, non-equal delay inverses for the same sequential machine, consider the machine M'' of Figure 1.3.

S'' \ X''	β	γ
$[s_4, \beta]$	$[s_4, \beta]$ a	$[s_5, \gamma]$ b
$[s_5, \gamma]$	$[s_4, \beta]$ b	$[s_5, \gamma]$ a

FIGURE 1.3 - FSM M'', A DELAY ONE INVERSE FOR M WITH RESPECT TO STATE s_4

Now both M' of Figure 1.2 and M'' of Figure 1.3 are inverses for M of Figure 1.1. The machine M' is a delay <u>two</u> inverse for M with respect to state s_1 while M'' is a delay <u>one</u> inverse for M with respect to s_4. We note that M'' is a delay one inverse for both s_4 and s_5 with initial state correspondence,

$s_4 \longleftrightarrow [s_4, \beta]$ and $s_5 \longleftrightarrow [s_5, \lambda]$, as we know from Theorem 1.1 since s_5 is reachable from s_4. However, M'' is not an inverse with respect to s_1 for any delay.

The machine of Figure 1.1 is one of a class of sequential machines for which an inverse exists with respect to every state. This follows from Theorem 1.1 since an inverse exists with respect to state s_1 and every state is reachable from state s_1. It is noted that the condition of Theorem 1.2 does not provide a convenient test for the existence of an inverse with given delay L since input sequences of every length $n \geq 1$ would have to be considered in order to verify that output sequences of length n + L are distinct for each length n input prefix. The following result, however, provides a test of finite length for existence of an inverse of given delay, and shows that the case n = 1 is the only one which must be considered if one examines all states reachable from s_0.

Theorem 1.3: An FSM M has a delay L inverse with respect to state s_0 if and only if

$$x \neq u \Rightarrow \lambda(s_i, x\, a^L) \neq \lambda(s_i, u\, b^L)$$

for every s_i reachable from s_0 and for every a^L and $b^L \in X^L$.

Proof: (Necessity) Suppose M' is a delay L inverse for M with respect to s_0. Suppose further that for some $x \neq u \in X$ and for some s_i reachable from s_0 we have $\lambda(s_i, x\, a^L) = \lambda(s_i, u\, b^L)$ for some a^L and $b^L \in X^L$. From Theorem 1.1 it follows that M has a delay L inverse with respect to s_i. But as a consequence

of Theorem 1.2 it is required that $\lambda(s_i,\ x\ a^L) \neq \lambda(s_i,\ u\ b^L)$ for $x \neq u$. Hence, a contradiction results and the stated condition is necessary for the existence of a delay L inverse with respect to s_0.

(Sufficiency) Suppose that the FSM M satisfies $\lambda(s_i,\ x\ a^L) \neq \lambda(s_i,\ u\ b^L)$ for every s_i reachable from s_0 and for every $x \neq u$ and a^L and $b^L \in X^L$. Suppose further that no delay L inverse exists for M with respect to state s_0. In this case, it follows from Theorem 1.2 that input sequences $x^n = x_1\ x_2 \cdots\cdots x_n$ and $u^n = u_1\ u_2 \cdots u_n$ can be found for some $n \geq 1$ such that $x^n \neq u^n$ and such that $\lambda(s_0,\ x^n\ c^L) = \lambda(s_0,\ u^n\ d^L)$ for some c^L and $d^L \in X^L$. Let i be the index of the first letter in which x^n and u^n differ. Let $s_j = \delta(s_0,\ x_1\ x_2 \cdots\cdots x_{i-1}) = \delta(s_0,\ u_1\ u_2 \cdots\cdots u_{i-1})$. But s_j is reachable from s_0 and $\lambda(s_j,\ x_i\ x_{i+1} \cdots\cdots x_n\ c^L) = \lambda(s_j,\ u_i\ u_{i+1} \cdots u_n\ d^L)$. Since $x_i \neq u_i$ we have a contradiction of the initial hypothesis. Consequently the assumption that no delay L inverse exists with respect to state s_0 is not compatible with the initial hypothesis and the theorem is proved.

Since the number of states on the sequential machines under study is finite, Theorem 1.3 defines a test of finite length for the existence of an inverse with a specified delay with respect to a particular state. The maximum length of the experiment necessary to show that an inverse does not exist is the subject of Chapter VIII which considers bounds on inverse delay. Other systematic tests for invertibility will be considered in Chapter III.

We now turn to the definition of certain output sequence, input sequence and state sets. These definitions will be useful in the discussion of various

structural properties of machines with inverses and will serve to make the proofs more concise. To this end we define the following.

Definition 1.3: The length n output sequence set for state s_i is given by

$$Y^n(s_i) = \left\{ y^n: \text{ There exists } x^n \text{ such that } \lambda(s_i, x^n) = y^n \right\}.$$

Definition 1.4: The initial state set for output sequence α^n is given by

$$S_i(\alpha^n) = \left\{ s : \alpha^n \in Y^n(s) \right\}.$$

Definition 1.5: The length n input sequence set for initial state s_i and output sequence α^n is given by

$$X^n(s_i, \alpha^n) = \left\{ x^n : \lambda(s_i, x^n) = \alpha^n \right\}.$$

Definition 1.6: The final state set for initial state s_i and output sequence α^n is given by

$$S_f(s_i, \alpha^n) = \left\{ s : \text{There exists } x^n \in X^n(s_i, \alpha^n) \text{ such that } \delta(s_i, x^n) = s \right\}.$$

Definition 1.7: The length n output sequence-final state pair set for state s_i is given by

$$F^n(s_i) = \left\{ (y^n, s) : y^n \in Y^n(s_i) \text{ and } s \in S_f(s_i, y^n) \right\}.$$

The sets given in Definitions 1.3 through 1.7 will be employed many times in the work which follows.

The sets defined by 1.5 and 1.6 imply a measure of uncertainty concerning possible input sequences and final states. Given an initial state s_0 and an output sequence α^n, the order of the length n input sequence set for s_0 and α^n is a

measure of the uncertainty concerning the input sequence which could have produced the output α^n. The order of the final state set for s_0 and α^n is a similar measure of uncertainty concerning the final state.

We shall be greatly concerned with the cardinalities and relations between the cardinalities of the various sets defined by 1.3 through 1.7. In particular, the implications of inverse existence on these set orders will be of interest. One such, rather obvious, relation between set orders is given as

Theorem 1.4:[2] If an FSM, M, has a delay L inverse with respect to state s_0 for some L, then $\#X^n(s_i, \alpha^n) = \#S_f(s_i, \alpha^n)$ for every s_i reachable from s_0 and for every $\alpha^n \in Y^n(s_i)$, $n \geq 0$.

Proof: Clearly $\#X^n(s_i, \alpha^n) \geq \#S_f(s_i, \alpha^n)$ for any machine. Suppose $\#X^n(s_i, \alpha^n) > \#S_f(s_i, \alpha^n)$ for some s_i reachable from s_0 and $\alpha^n \in Y^n(s_i)$. It follows that there exist $a^n \neq b^n \in X^n$ and $s_n \in S_f(s_i, \alpha^n)$ such that both $\lambda(s_i, a^n) = \lambda(s_i, b^n) = \alpha^n$ and $\delta(s_i, a^n) = \delta(s_i, b^n) = s_n$. But then $\lambda(s_i, a^n x^k) = \lambda(s_i, b^n x^k)$ for every $x^k \in X^k$; $k \geq 0$. Since $a^n \neq b^n$ it follows that there exists some state s_j reachable from s_i (and thus from s_0) such that $\lambda(s_j, xc^L) = \lambda(s_j, ud^L)$ for $x \neq u$. By Theorem 1.3 M does not have a delay L inverse with respect to s_0 for any L and the theorem follows.

[2]It can be shown that the assertion of this theorem holds for a somewhat weaker condition, i.e., the information lossless condition to be considered in Chapter III.

Another result which can be proved quite easily as a consequence of requirements on the order of the length n output sequence set for any state s_i is the following.

Theorem 1.5: An FSM has no inverse with respect to any state if $\#X > \#Y$.

Proof: Suppose for some FSM M we have $\#X = q$ and $\#Y = p$. Suppose further that $q > p$. If a delay L inverse for M exists with respect to state s_i we have as a direct consequence of Theorem 1.2 that $\#Y^{n+L}(s_i) \geq q^n$ for every $n \geq 1$. But there can exist at most p^{n+L} output sequences of length n + L. Hence, $\#Y^{n+L}(s_i) \leq p^{n+L}$. It follows that $p^{n+L}/q^n \geq 1$. However, consider the behavior of p^{n+L}/q^n as n increases without limit. We have

$$\lim_{n \to \infty} \left[p^{n+L}/q^n\right] = p^L \lim_{n \to \infty} \left[p^n/q^n\right] = 0$$

since $q > p$. Therefore, the existence of an inverse for M requires that $q \leq p$.

As a consequence of the previous result we may state an additional necessary condition on the union of the length n output sequence sets. It is possible to show that if a sequential machine has an inverse, then a certain number of distinct output sequences of every length must exist. The necessary condition is given as

Theorem 1.6: If an FSM M has a delay L inverse with respect to state s_0 for some L and if $\#X = q$, then for any $j \geq 0$

$$\#\left\{ \bigcup_{\substack{s_i \text{ reachable} \\ \text{from } s_0}} Y^j(s_i) \right\} \geq q^j .$$

Proof: Consider the FSM $M^j(s_0) = \langle S^*, X^*, Y^*, \delta^*, \lambda^* \rangle$ which is the j-th extension of M with respect to state s_0 and is defined by

$$S^* = \{ s_i : \text{there exists } x^{nj} \text{ such that } \delta(s_0, x^{nj}) = s_i;\ n \geq 1 \}$$

$$X^* = X^j$$

$$Y^* = \{ y^j : \text{there exists } s_i \in S^* \text{ and } x^j \text{ such that } \lambda(s_i, x^j) = y^j \}$$

$$\delta^*(s_i, x^j) = \delta(s_i, x^j)$$

$$\lambda^*(s_i, x^j) = \lambda(s_i, x^j)$$

Suppose $\#\left\{ \bigcup_{\substack{s_i \text{ reachable} \\ \text{from } s_0}} Y^j(s_i) \right\} < q^j$.

This implies that $\#Y^* < q^j = \#X^j = \#X^*$. By Theorem 1.5 no inverse with any delay exists for $M^j(s_0)$ with respect to any state. However, if M has a delay L inverse with respect to state s_0 for some L, then it follows that the j-th extension of M' with respect to s_0', $M'^j(s_0)$, is also an inverse for $M^j(s_0)$. Hence, if M has an inverse with respect to s_0, the assertion of the theorem follows.

In the special case for which #X = #Y, the result of Theorem 1.6 may be extended by the following two corollaries.

Corollary 1.6.1: If an FSM M has a delay L inverse with respect to state s_0 for some L and if #X = #Y = q, then for every $j \geq 0$

$$\#\left\{ \bigcup_{\substack{s_i \text{ reachable} \\ \text{from } s_0}} Y^j(s_i) \right\} = q^j .$$

Proof: If #Y = q it follows that

$$\#\left\{ \bigcup_{\substack{s_i \text{ reachable} \\ \text{from } s_0}} Y^j(s_i) \right\} \leq \#\left\{ \bigcup_{s_i \in S} Y^j(s_i) \right\} \leq q^j .$$

Since M has an inverse with respect to state s_0, Theorem 1.6 requires that

$$\#\left\{ \bigcup_{\substack{s_i \text{ reachable} \\ \text{from } s_0}} Y^j(s_i) \right\} \geq q^j \quad .$$

Hence, it must be that

$$\#\left\{ \bigcup_{\substack{s_i \text{ reachable} \\ \text{from } s_0}} Y^j(s_i) \right\} = q^j \quad .$$

Corollary 1.6.2: If an FSM M has a delay L inverse with respect to state s_0 for some L and if #X = #Y = q, then for every $j \geq 0$ and for every y^j, there exists some state, say s_i, reachable from s_0 such that $y^j \in Y^j(s_i)$.

Proof: The proof follows trivially from Corollary 1 since if there exists some output sequence y^j for some j such that $y^j \notin Y^j(s_i)$ for any s_i reachable from s_0, then

$$\#\left\{ \bigcup_{\substack{s_i \text{ reachable} \\ \text{from } s_0}} Y^j(s_i) \right\} \leq q^j - 1$$

and the condition of Corollary 1 is not satisfied.

This concludes the preliminary results of Chapter I. In this chapter we have presented a very general inverse definition pertaining to the general class of finite state machines. Some implications of inverse existence were investigated, necessary and sufficient conditions for inverse existence were obtained, and some requirements on certain input, output and state set orders were derived. In the next chapter we will modify our inverse definition to some extent and show some interesting properties of a more restricted class of FSM's for which an inverse exists according to this modified definition.

CHAPTER II

GENERAL DELAY L INVERSES

In this and in succeeding chapters we will make use of a modification of the inverse definition given in Chapter I. An FSM M' will be considered a general delay L inverse for an FSM M if M' is a delay L inverse with respect to all states. Formally we will consider the following.

Definition 2.1: An FSM M' is a general delay L inverse for an FSM M if M' is a delay L inverse for M with respect to s for every $s \in S$.

Furthermore, it will often be necessary to consider the least integer L for which an FSM has a general delay L inverse. For convenience we shall say that M is INV #L if L is the least integer for which M has a general delay L inverse. Moreover, we shall say that M is invertible if M is INV#L for some integer L. Invertibility will be considered in this sense in all that follows.

In this chapter some structural properties of a certain class of invertible finite state machines will be investigated. A necessary and sufficient condition for machines of this class to possess the INV #L property will also be presented. The class of FSM's to be considered is defined by two constraints; strong connectedness and equal order input and output alphabets.

Definition 2.2: An FSM is strongly connected if, for all possible pairs of states s_i and s_j, there exists some input sequence x^n for some n such that $\delta(s_i, x^n) = s_j$.

It is clear, in the case of strongly connected machines, that an inverse with delay L with respect to any state implies the existence of a general delay L inverse. This follows immediately from Theorem 1.1 since every state is reachable from every other state if strong connectedness holds.

The two characteristics of strong connectedness and #X = #Y together with the invertible condition yield some interesting results concerning the structural properties of FSM's of this class. One of these results is given as

Theorem 2.1: If M is a strongly connected, INV #L FSM with #X = #Y = q, then $\#S_f(s, y^n) = J$ for some J, for every $s \in S$, for every $y^n \in Y^n(s)$ and for every $n \geq L$.

Proof: Let s_i and α^L satisfy

$$\#S_f(s_i, \alpha^L) = \underset{s \in S,\ y^L \in Y^L(s)}{\text{MAX}} \#S_f(s, y^L)$$

and in addition, define $J = \#S_f(s_i, \alpha^L)$. Suppose there exist s_j and β^n with $n \geq L$ such that $\#S_f(s_j, \beta^n) \neq J$. From the strongly connected property there exists γ^k for some k such that $s_j \in S_f(s_i, \alpha^L \gamma^k)$. But if M is INV #L it follows that the sequence $\alpha^L \gamma^k \beta^n$ implies the (k + n)-th successor of s_i, say s_k. Let ρ^L be the last L letters of β^n. Consequently, we may write $S_f(s_i, \alpha^L \gamma^k \beta^n) = S_f(s_j, \beta^n) = S_f(s_k, \rho^L)$, which in turn implies that $\#S_f(s_k, \rho^L) < J$ since J is maximum over all such state sets and $\#S_f(s_j, \beta^n) \neq J$. But Theorem 1.4 implies that

$$\sum_{y^{k+n} \in Y^{k+n}} \#X^{L+k+n}(s_i, \alpha^L y^{k+n}) = \sum_{y^{k+n} \in Y^{k+n}} \#S_f(s_i, \alpha^L y^{k+n}) = q^{k+n} \cdot J.$$

Hence, since #X = #Y = q and since $\#S_f(s_i, \alpha^L \gamma^k \beta^n) < J$, there must exist some σ^{k+n} such that $\#S_f(s_i, \alpha^L \sigma^{k+n}) > J$. But the INV #L property again requires that $\alpha^L \sigma^{k+n}$ implies the (k+n)-th successor state of s_i, say s_n. Let η^L be the sequence containing the last L letters of σ^{k+n}. It follows that $S_f(s_i, \alpha^L \sigma^{k+n}) = S_f(s_n, \eta^L)$ and hence that $\#S_f(s_n, \eta^L) > J$. Therefore, J is not maximum as was assumed and by contradiction the theorem follows.

The result of Theorem 2.1 requires that, for the class of FSM's considered, the observation of any output sequence of length L or longer from any known initial state yields the same uncertainty regarding the final state. The order of the final state set is the same for any choices of initial state s_i and output sequence of length L or longer allowed by s_i.[1] By Theorem 1.4, it is clear that this result may also be extended to show that the length n input sequence sets all have common order.

Another quite similar result concerning the order of the length n output sequence sets for $n \geq L$ can be shown. In this case we may state

Theorem 2.2: If M is a strongly connected, INV #L FSM with #X = #Y = q, then $\#Y^n(s) = q^n/J$ for every $s \in S$ and $n \geq L$.

Proof: As a result of Theorem 2.1 we have $\#S_f(s, y^n) = J$ for $n \geq L$ and $y^n \in Y^n(s)$. By Theorem 1.4 we have $\#S_f(s, y^n) = \#X^n(s, y^n)$. But it is always true that

$$\sum_{y^n \in Y^n(s)} \#X^n(s, y^n) = q^n \quad .$$

Hence, $\#Y^n(s) \cdot \#X^n(s, y^n) = \#Y^n(s) \cdot J = q^n$. Consequently, $\#Y^n(s) = q^n/J$.

[1] We say that a state s_i allows the output sequence y^n if there exists x^n such that $\lambda(s_i, x^n) = y^n$.

Since the number of distinct output sequences of any length must be an integer, it follows that J divides q^n. In the special case in which q is prime we have the following corollary.

Corollary 2.2.1: If an FSM M satisfies the hypothesis of Theorem 2.2 and if, in addition, q is prime, then for every $n \geq L$, for every $s \in S$ and $y^n \in Y^n(s)$ there exists some integer j such that $\#S_f(s, y^n) = \#X^n(s, y^n) = q^j$ and $\#Y^n(s) = q^{n-j}$.

Proof: When q is prime the requirement that J divide q^n for every $n \geq L$ implies that $J = q^j$ for some j. The corollary follows.

The preceding two results of Theorems 2.1 and 2.2 illustrate important structural properties of strongly connected, invertible machines with the same input and output set orders. For example, if M is a binary input, binary output, INV #4 FSM, then the number of output sequences of length four allowed by any state must be the same power of two, say 2^k, for some $k < 4$. If, for instance, any state allows precisely three sequences of length four, then no delay four inverse exists. Furthermore, we have that $\#S_f(s, y^n)$ is the same power of two or 2^{4-k} for every $s \in S$ and $y^n \in Y^n(s)$ if $n \geq 4$. Hence, uncertainty is preserved and output sequences of length four or longer do not yield differing uncertainties regarding the applied input sequences.

These highly restrictive structural properties tend to limit the number of invertible, strongly connected FSM's with #X = #Y. Although no enumeration of such machines will be attempted for specified input, output and state set

orders it is apparent that these machines form a small part of the set of all such FSM's.

Our final result of this chapter will be a necessary and sufficient condition for a strongly connected FSM with #X = #Y to be INV #L. The proof of this result will incorporate the following lemma.

Lemma 2.1: If M is an INV #L FSM, then $\left\{Y^n(s_i) \bigcap Y^n(s_j)\right\} = \phi$ (the empty set) for every $n \geq L$ and for every $s_i,\ s_j \in S_f(s,\ y^L)$ for any $s \in S$ and $y^L \in Y^L(s)$.

Proof: The proof follows directly from the definition of an INV #L machine.

Lemma 2.1 states that no two states in any final state set for any initial state and length L output sequence can allow a common output sequence of length L or longer. Making use of the lemma and of Theorems 2.1 and 2.2 it is possible to show

Theorem 2.3: If an FSM M is strongly connected and #X = #Y, then M is INV #L if and only if for every $s_i \in S$ and $\alpha^L \in Y^L(s_i)$

$$\bigcup_{s \in S_f(s_i,\ \alpha^L)} Y^n(s) = Y^n$$

for every $n \geq 0$.

Proof: We first consider necessity. By Lemma 2.1 it follows that

$$\#\left\{\bigcup_{s \in S_f(s_i,\ \alpha^L)} Y^n(s)\right\} = \sum_{s \in S_f(s_i,\ \alpha^L)} \#Y^n(s)$$

for $n \geq L$. This follows since no two states in $S_f(s_i,\ \alpha^L)$ can allow the same

length n output sequence. The results of Theorems 2.1 and 2.2 further imply that

$$\sum_{s \in S_f(s_i, \alpha^L)} \#Y^n(s) = q^n = \#\left\{Y^n\right\}.$$

Hence, it must be that

$$\bigcup_{s \in S_f(s_i, \alpha^L)} Y^n(s) = Y^n.$$

Clearly the necessity of the above result for $n \geq L$ implies the result must also hold for $n \geq 0$. Consequently, necessity is shown for all $n \geq 0$.

We next prove sufficiency. To do this we assume that

$$\bigcup_{s \in S_f(s_i, \alpha^L)} Y^n(s) = Y^n$$

for every $n \geq 0$, for every s_i and $\alpha^L \in Y^L(s_i)$ and show that M is INV #L. Let

$$J = \underset{s \in S,\ y^L \in Y^L(s)}{\text{MIN}} \#S_f(s, y^L)$$

and let s_j and β^L satisfy $\#S_f(s_j, \beta^L) = J$. It follows from our initial assumption and from the fact that #X = #Y that $\#S_f(s_j, \beta^L y^n) = J$ for every n and for every y^n. If this property does not hold, then there must exist some successor of s_j and some length L output sequence such that the corresponding final state set has order less than J; a result which contradicts our hypothesis that J is minimum over all such state sets. Suppose M is not INV #L. This implies that there exists $s_0 \in S$ and $a^{L+1} = a_1\ a_2 \cdots a_{L+1}$ and $b^{L+1} = b_1\ b_2 \cdots b_{L+1}$ such that $a_1 \neq b_1$ and such that $\lambda(s_0, a^{L+1}) = \lambda(s_0, b^{L+1}) = \gamma_1\ \gamma_2 \cdots \gamma_{L+1}$. Since M is strongly connected, there exists some output sequence, ρ^k, for some $k \geq 0$ such that $s_0 \in S_f(s_j, \beta^L \rho^k)$. However, $\#S_f(s_0, \gamma_1\ \gamma_2 \cdots \gamma_L \geq J$

and $\#S_f(s_0, \gamma_1 \gamma_2 \cdots \gamma_L) > J$ implies that $\#S_f(s_j, \beta^L \rho^k \gamma_1 \gamma_2 \cdots \gamma_L) > J$. But this is a contradiction of our earlier conclusion that $\#S_f(s_j, \beta^L y^n) = J$ for every y^n and every n. Hence, we conclude that $\#S_f(s_0, \gamma_1 \gamma_2 \cdots \gamma_L) = J$. Since

$$\bigcup_{s_k \in S_f(s_0, \gamma_1 \gamma_2 \cdots \gamma_L)} Y(s_k) = Y$$

and since $\gamma_2 \gamma_3 \cdots \gamma_{L+1} \in \left\{ Y^L(\delta(s_0, a_1)) \bigcap Y^L(\delta(s_0, b_1)) \right\}$, it follows that either $\#S_f(\delta(s_0, a_1), \gamma_2 \gamma_3 \cdots \gamma_{L+1}) < J$ or $\#S_f(\delta(s_0, b_1), \gamma_2 \gamma_3 \cdots \gamma_{L+1}) < J$. Consequently, J is not the minimum order of such a final state set and we conclude from the contradiction that if M is not INV #L, then

$$\bigcup_{s \in S_f(s_i, \alpha^L)} Y^n(s) \neq Y^n$$

and the theorem is proved.

The result of Theorem 2.3 means that, for the class of FSM's considered, it is possible to choose arbitrarily an output sequence of any length and find a state that allows the chosen output sequence in any final state set of the form, $S_f(s, y^L)$. Stated another way, it is possible to generate from any initial state an arbitrarily selected output sequence of any length after a transient period of at most L time units.

In this chapter we have defined notions of invertibility, of general delay L inverses and of INV #L machines. We have considered these definitions as applied to the class of strongly connected FSM's with the same input and output set orders. Several structural properties of INV #L machines of this class were obtained and a necessary and sufficient condition for INV #L behavior was proved. In the next chapter we will consider some concepts of invertibility and some tests for inverse existence defined by previous investigators and relate these to our work.

CHAPTER III

INFORMATION LOSSLESSNESS

Information losslessness and information losslessness of finite order were first defined and studied by Huffman[1,2]. The latter property, as will be shown, is quite similar to our INV #L condition as given in Chapter II. Following Huffman we may state

Definition 3.1: An FSM is information lossless (IL) if there exists no state s_i and no two distinct input sequences x^n and u^n; $n \geq 1$; such that both $\lambda(s_i, x^n) = \lambda(s_i, u^n)$ and $\delta(s_i, x^n) = \delta(s_i, u^n)$.

Definition 3.2: An FSM is information lossless of finite order N (ILF of order N if for every pair of length N+1 input sequences with different first letters x^{N+1} and u^{N+1}, there exists no state s_i such that $\lambda(s_i, x^{N+1}) = \lambda(s_i, u^{N+1})$.

Machines which are ILF of order N satisfy the property that knowledge of the initial state and first N+1 output letters guarantees the decipherment of the first input letter. Machines which are INV #L according to our definition also require L+1 output letters in order to guarantee this result. However, the class of ILF of order N machines includes the N-1, N-2, ····· and zeroeth order classes whereas an INV #L machine is not INV #(L-k) for any $k \geq 1$. The

[1] D. A. Huffman, "Information Conservation and Sequence Transducers," Proceedings Symposium on Information Networks, Polytechnic Institute of Brooklyn, April 1954, pp. 291-307.

[2] D. A. Huffman, "Canonical Forms for Information Lossless Finite State Logical Machines," Transactions of the IRE Professional Group on Circuit Theory, Vol. CT-6 Special Supplement, May 1959, pp. 41-59.

relationship between the INV #L property of Chapter II and that of information losslessness of finite order as in Definition 3.2 is thus that

Theorem 3.1: An FSM M is INV #L if and only if L is the least integer such that M is ILF of order L.

Proof: If M is INV #L, then by Theorem 1.3 and Definition 2.1 there can exist no two input sequences of length L+1 which differ in the first letter and which yield the same output sequence from any initial state. Hence M satisfies Definition 3.2 and is therefore ILF of order L. Conversely, if M is ILF of order L, Theorem 1.3 is satisfied for every initial state and M has a general delay L inverse. Since L is the least integer such that M has a general delay L inverse, it follows that M is INV #L.

As indicated by Huffman the more general class of IL machines are not invertible. It is interesting to note, however, that in the case of minimal, IL FSM's, it is possible to determine for any n, the applied input sequence of length n from knowledge of the initial state and length n output sequence by a suitable terminal state identification experiment. As shown by Gill[3] such identification experiments always exist in the case of minimal machines. Terminal state identification experiments consist of the application of an input sequence which yields a known terminal state no matter which of the states of $S_f(s_i, \alpha^n)$ that the FSM occupies after observation of the output sequence α^n from initial state s_i. The relevance of the term, "information losslessness",

[3]A. Gill, Introduction to the Theory of Finite State Machines. McGraw-Hill, 1962, pp. 123-125, 149-153.

is apparent. Input information can always be recovered in some sense. In certain cases another interesting characterization of IL machines is possible as we will see shortly (Theorem 3.3).

First let us consider the inclusion properties of IL and ILF machines. The following, rather obvious, theorem is due to Even[4].

Theorem 3.2: If an FSM is ILF (and hence invertible), then it is also IL.

The converse of Theorem 3.2 is not true however, as is well known. This can be shown by counter example. The machine of Figure 3.1 is such a counter example.

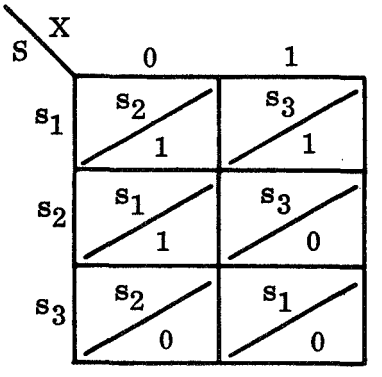


FIGURE 3.1 - A BINARY, IL, BUT NOT ILF FSM

The fact that the machine of Figure 3.1 is IL but is not ILF is most easily determined by a testing procedure which we shall now describe.

Several testing procedures for the determination of IL and ILF properties are available in the literature, e.g., Huffman[2], Even[4] or Hennie[5]. A most

[4]S. Even, "On Information Lossless Automata of Finite Order", IEEE Transactions on Electronic Computers, EC 14, August 1965, pp. 561-569.

[5]F. Hennie, Finite State Models for Logical Machines, John Wiley & Sons, 1968.

efficient test is due to Even and incorporates in one simple procedure a test for both IL and ILF conditions. Even's procedure can be summarized as follows:

(1) Consider the possible paths on the state transition diagram which leave a given state with common output labels. Construct an "invertibility test graph" (ITG) by taking all such paths two at a time labelling successive nodes on the ITG with the pairs of states at the same depth from the given state. The state pairs labelling each node on the graph are called compatible pairs. More precisely,

Definition 3.3: Two states s_i and s_j are a compatible pair (s_i, s_j) if either:

(i) there exists a state s_k and input letters x and u such that

$$\delta(s_k, x) = s_i, \qquad \delta(s_k, u) = s_j$$

and $$\lambda(s_k, x) = \lambda(s_k, u)$$

or (ii) there exists a compatible pair (s_n, s_m) and input symbols x and u such that

$$\delta(s_n, x) = s_i, \qquad \delta(s_m, u) = s_j$$

and $$\lambda(s_n, x) = \lambda(s_m, u) \ .$$

(2) M is IL if and only if the ITG for M contains no compatible pairs of the form (s_i, s_i) for any $s_i \in S$.

(3) M is ILF of order N if and only if the ITG for M is loop free and the longest chain of compatible pairs (nodes) on the ITG has not more than N nodes.

To illustrate the application of this test, consider the machine of Figure 3.1 and corresponding ITG of Figure 3.2.

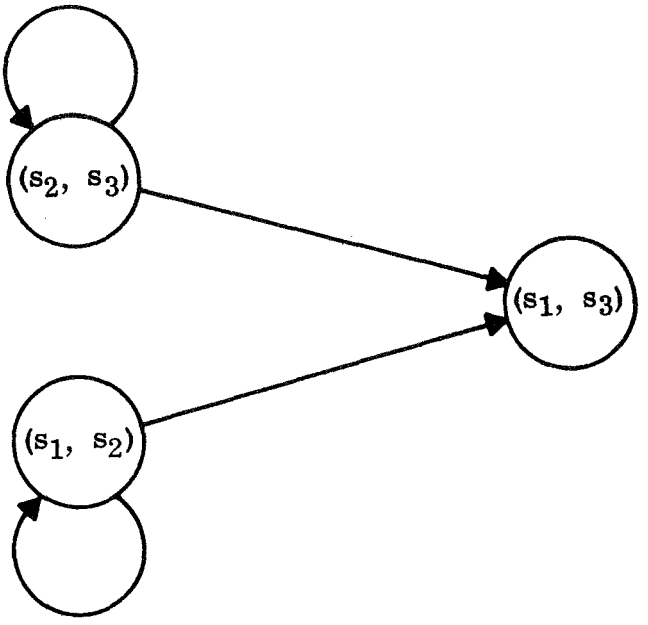


FIGURE 3.2 - THE INVERTIBILITY TEST GRAPH FOR THE FSM OF FIGURE 3.1

The complete ITG shown in Figure 3.2 has no pairs for the form (s_i, s_i). Hence, the FSM of Figure 3.1 is IL. However, the ITG is not loop free since both nodes (s_2, s_3) and (s_1, s_2) close on themselves. Therefore, the FSM is not ILF and hence is not invertible.

The number of compatible pairs of states which appear on the ITG for any FSM M may be found by consideration of all distinct pairs of states in the final state sets for M. This conclusion results from the following lemma.

Lemma 3.1: For any FSM M, if s_i and $s_j \in S_f(s_k, \alpha^n)$ for some s_k and α^n, then (s_i, s_j) is a compatible pair on the ITG for M. Conversely if (s_i, s_j) is a compatible pair on the ITG for M, then there exist s_k and α^n for some n such that both s_i and $s_j \in S_f(s_k, \alpha^n)$.

Proof: The proof follows directly from Definitions 1.6 and 3.3.

We now turn to the additional characterization of a certain class of information lossless machines which was alluded to earlier. Our restriction here will be to the same class of FSM's considered in Chapter II, viz, those possessing strong connectedness and satisfying #X = #Y.

Theorem 3.3:[6] If M is a strongly connected FSM with #X = #Y, then M is IL if and only if

$$\bigcup_{s \in S} Y^n(s) = Y^n$$

for every $n \geq 0$.

Proof: First we consider sufficiency. To prove sufficiency we will show that if M is not IL, then there exists some y^n for some $n \geq 1$ such that y^n is not allowed by any state. To accomplish this we make use of

Lemma 3.2: If a strongly connected FSM is not IL, then there exists an integer $n \geq 1$ such that for every $s \in S$ and for every $m \geq n$ there exists $x^m \neq u^m$ such that $\delta(s, x^m) = \delta(s, u^m)$ and $\lambda(s, x^m) = \lambda(s, u^m)$.

Proof: The hypothesis that M is not IL implies the existence of s_0 and $s_f \in S$ and $a^i \neq b^i \in X^i$ for some i such that $\delta(s_0, a^i) = \delta(s_0, b^i) = s_f$ and $\lambda(s_0, a^i) = \lambda(s_0, b^i)$. By the strong connectedness property there exists v^j for some

[6]The result embodied in this theorem has been previously shown within the framework of Graph Theory. See: L. R Welch, "Labelled Oriented Graphs which are Onto", N.S.A. Technical Journal, October 1966, pp. 43-49.

$j \leq N-1$ (where $N = \#S$) for every $s \in S$ such that $\delta(s, v^j) = s_0$. Let $x^n = v^j a^i$ and let $u^n = v^j b^i$. Clearly $n \leq N-1 + i$ and $\delta(s, x^n) = \delta(s, u^n)$ and $\lambda(s, x^n) = \lambda(s, u^n)$. Since the final state is the same for both x^n and u^n it follows that $x^m = x^n w^k$ and $u^m = u^n w^k$, where w^k is any input sequence whatever, satisfies the assertion of the lemma.

Consider the length k output sequence - final state pair for state s set, $F^k(s)$, given as in Definition 1.7;

$$F^k(s) = \left\{ (y^k, s_k): \text{ There exists } x^k \text{ such that } \delta(s, x^k) = s_k \text{ and } \lambda(s, x^k) = y^k \right\}.$$

By Lemma 3.2 it follows that for every $s \in S$ there exists some n such that for every $m \geq n$ we have $\#F^m(s) \leq q^m - 1$ (where $q = \#X = \#Y$). This follows since each pair (y^m, s_m) in $F^m(s)$ must result from a distinct input sequence of length m and at least two of the possible q^m input sequences yield the same pair.

It can be easily verified that for every k, $j \geq 1$ and for every $s \in S$

$$F^{k+j}(s) = \left\{ (y^k y^j, s_f): \text{ there exists } s_k \text{ such that } (y^k, s_k) \in F^k(s) \text{ and } (y^j, s_f) \in F^j(s_k) \right\}.$$

Making use of this representation for $F^{k+j}(s)$ it is possible to state

Lemma 3.3: $\#F^{k+j}(s) \leq \#F^k(s) \cdot \underset{k}{\text{MAX}} \#F^j(s_k)$.

Proof: The proof of the lemma follows from the fact that

$$\#F^{k+j}(s) \leq \# \left\{ \left[(y^k, s_k), (y^j, s_f)\right] : (y^k, s_k) \in F^k(s) \text{ and } (y^j, s_f) \in F^j(s_k) \right\}.$$

Inequality is possible in the above expression since more than one state s_k may be associated with a fixed choice of y^k, y^j and s_f. Clearly if we choose s_k such that $\#F^j(s_k)$ is maximum, then $\#F^{k+j}(s) \leq \#F^k(s) \cdot \#F^j(s_k)$ and the lemma is proved.

Applying the result of Lemma 3.3 for j = m and recalling that $\#F^m(s_k) \leq q^m - 1$ we have for the machine M

$$\#F^{k+m}(s) \leq \#F^k(s) \cdot (q^m - 1)$$

for every k and for every $s \in S$. As a consequence it follows that for any $t \geq 1$

$$\#F^{tm}(s) \leq (q^m - 1)^t$$

which further implies that

$$\sum_{s \in S} \#F^{tm}(s) \leq N \cdot (q^m - 1)^t \ .$$

Suppose, on the other hand, that for any choice of y^n for any n there exists some state in S which allows y^n. This is equivalent to

$$\bigcup_{s \in S} Y^n(s) = Y^n \ .$$

For n = tm we have that

$$\bigcup_{s \in S} Y^{tm}(s) = Y^{tm} \ .$$

Hence, it must be that

$$\sum_{s \in S} \#Y^{tm}(s) \geq q^{tm} \ .$$

But it is always true that

$$\#Y^n(s) \leq \#F^n(s) \ .$$

Therefore, we have

$$\sum_{s \in S} \#F^{tm}(s) \geq q^{tm} \ .$$

By combination of the upper and lower bounds on the summation $\sum_{s \in S} \#F^{tm}(s)$, it follows that

$$q^{tm} \leq N \cdot (q^m - 1)^t$$

and hence that

$$N \geq (q^m/(q^m - 1))^t$$

for every t. The result is clearly not possible since the right hand side is unbounded as t increases without limit and N must be finite. Therefore, we conclude that if M is not IL, then there exists some n and some output sequence y^n such that y^n is not allowed by any state. Hence, sufficiency of the condition of the theorem for the IL property is shown.

To show necessity we assume that there exists some n and some $\alpha^n \in Y^n$ such that α^n is not allowed by any state and show that M is not IL. Suppose M is IL. It follows from Definition 3.1 that $(y^{kn}, s_f) \in F^{kn}(s)$ implies the applied input sequence x^{kn} for every $s \in S$. Hence, it must be that $\#F^{kn}(s) \geq q^{kn}$. But if α^n is not allowed by any state it follows that $\#Y^n(s) \leq q^n - 1$ and further that $\#Y^{kn}(s) \leq (q^n - 1)^k$ for every $k \geq 1$. In addition, for $N = \#S$ we have that $\#F^{kn}(s) \leq N \cdot \#Y^{kn}(s) \leq N \cdot (q^n - 1)^k$. Combining the upper and lower bounds on $\#F^{kn}(s)$ the result is

$$N \cdot (q^n - 1)^k \quad q^{nk}$$

which yields

$$N \geq (q^n/(q^n - 1))^k$$

for every k. Since N must be finite this result is not possible as was concluded also in the proof of sufficiency. Hence, the assumption that α^n is not allowed by any state implies that M is not IL and necessity is shown.

The condition of Theorem 3.3 for the IL property may be compared with the similar result of Theorem 2.3 for invertibility or the INV #L property. The same class of FSM's is considered in each case, viz, strongly connected machines with the same input and output set orders. Both invertibility and information-losslessness imply that one can arbitrarily choose an output sequence of any length and find a state which allows that sequence. Invertibility, being a stronger property, however, requires that such a state be reachable in at most L time units where L is the inverse delay. Hence, for INV #L machines, any desired response can be obtained after a transient period of length L.

Consideration of the IL property for general FSM's leads naturally to questions concerning bounds. In particular, we may inquire as to the maximum integer n such that there exists no state s or input sequences $x^n \neq u^n$ satisfying $\delta(s, x^n) = \delta(s, u^n)$ and $\lambda(s, x^n) = \lambda(s, u^n)$ on a non-IL machine. We are able to derive an upper bound on this integer for the general class of FSM's. The bound is given by

Theorem 3.4: If an FSM M is not IL, then there exists s_0 and $a^n \neq b^n$ such that $\lambda(s_0, a^n) = \lambda(s_0, b^n)$ and $\delta(s_0, a^n) = \delta(s_0, b^n)$ for some $n \leq \binom{N}{2} + 1$ where N = #S.

Proof: Let M be any non-IL FSM. Suppose the least integer n such that there exist s_0, a^n and b^n satisfying the assertion of the theorem is greater than $\binom{N}{2} + 1$. Let $a^n = a_1\, a_2 \cdots a_n$ and $b^n = b_1\, b_2 \cdots b_n$. Since there are only

$\binom{N}{2}$ possible distinct pairs of distinct states it follows that for some i, j; $i < j \leq \binom{N}{2}$; we have either

$$\delta(s_0,\ a_1\ a_2 \cdots\cdots a_i) = \delta(s_0,\ a_1\ a_2 \cdots a_j) \quad \text{and}$$

$$\delta(s_0,\ b_1\ b_2 \cdots\cdots b_i) = \delta(s_0,\ b_1\ b_2 \cdots b_j)$$

or

$$\delta(s_0,\ a_1\ a_2 \cdots a_i) = \delta(s_0,\ b_1\ b_2 \cdots b_j) \quad \text{and}$$

$$\delta(s_0,\ b_1\ b_2 \cdots b_i) = \delta(s_0,\ a_1\ a_2 \cdots a_j)\ .$$

In either case it is clear, since $\delta(s_0, a^n) = \delta(s_0, b^n)$ and $\lambda(s_0, a^n) = \lambda(s_0, b^n)$, that there exist input sequences of length n-j, say c^{n-j} and d^{n-j}, such that

$$\delta(s_0,\ a_1\ a_2 \cdots a_i\ c^{n-j}) = \delta(s_0,\ b_1\ b_2 \cdots b_i\ d^{n-j})$$

and

$$\lambda(s_0,\ a_1\ a_2 \cdots a_i\ c^{n-j}) = \lambda(s_0,\ b_1\ b_2 \cdots b_i\ d^{n-j})\ .$$

But $i < j$. Hence, $i + n-j < n$ and n is not the least integer such that the assertion of the theorem is true. Consequently, it follows that the minimum such integer is less than $\binom{N}{2} + 1$.

Theorem 3.3 implies that there exists some maximum integer n such that for every y^n one can find s and x^n satisfying $\lambda(s, x^n) = y^n$ on a non-IL, strongly connected FSM with N states and #X = #Y = q. We are not able to give a satisfactory bound on this integer n. A very loose upper bound on n which follows from Lemma 3.2 and Theorem 3.4 and which is given in terms of N and q has been obtained. The bound grows rapidly with N however, and is not considered of sufficient consequence to present here. We remark that, in the case of binary machines, a tight bound on n appears to be given by $n \leq 2\ (N-1)$. We have not been able to prove this conjectured bound for the binary case, however.

We present in this Chapter one more result which is closely associated with the work of Hennie[5]. Hennie defines a test for the ILF property which, in terms of our parameters, consists basically of a test on the order of the intersection of initial state sets and final state sets. A slight extension and simplification of Hennie's procedure is presented in the following result.

Theorem 2.6: An IL finite state machine M is INV #L if and only if L is the least integer such that

$$\#\left\{ S_f(s_i, \alpha) \cap S_i(\beta^L) \right\} < 2$$

for every $s_i \in S$, $\alpha \in Y(s_i)$ and $\beta^L \in Y^L$.

Proof: First consider the sufficiency of the condition given in the theorem. Suppose that

$$\#\left\{ S_f(s_i, \alpha) \cap S_i(\beta^L) \right\} < 2$$

for every $s_i \in S$, $\alpha \in Y(s_i)$ and $\beta^L \in Y^L$ for some least integer L. Two possibilities exist. Either

$$\#\left\{ S_f(s_i, \alpha) \cap S_i(\beta^L) \right\} = 0$$

or

$$\#\left\{ S_f(s_i, \alpha) \cap S_i(\beta^L) \right\} = 1 \quad .$$

Since M is IL, by Definition 3.1 there exist no two input letters, $x \neq u$ for any $s_i \in S$ such that

$$\lambda(s_i, x) = \lambda(s_i, u)$$

and

$$\delta(s_i, x) = \delta(s_i, u) \quad .$$

Therefore, for any s_i there exists at most one input letter, x, such that

$$\lambda(s_i, x) = \alpha$$

and

$$\delta(s_i, x) \in S_i(\beta^L)$$

for any $\alpha \in Y(s_i)$ and $\beta^L \in Y^L$.

By Definition 3.2 M is ILF of order L and by Theorem 3.1 M is INV #L. Consider the necessity of the condition given in the theorem. Suppose there exists no L such that

$$\# \left\{ S_f (s_i, \alpha) \cap S_i (\beta^L) \right\} < 2$$

for every s_i, α and β^L. It follows that for every L there exists some s_i and two input letters $x \neq u$ such that

$$\lambda(s_i, x) = \lambda(s_i, u) = \alpha \ ,$$

$$\delta(s_i, x) \in S_i (\beta^L) \text{ and } \delta(s_i, u) \in S_i (\beta^L)$$

for some $\alpha \in Y$ and $\beta^L \in Y^L$. Clearly then

$$\lambda(s_i, x\, a^L) = \lambda(s_i, u\, b^L) = \alpha \beta^L$$

for some a^L and $b^L \in X^L$. By Definition 3.2 M is not ILF of order L and by Theorem 3.1 M is not INV #L.

An application of the result of Theorem 3.5 to test for ILF properties and consequently for invertibility differs from the test of Hennie in that in our test it is necessary to consider final state sets, $S_f (s_i, \alpha)$ for sequences, α, of length only one. The formulation of the forward test table of Hennie's work requires that the table be extended to include all possible distinct sets $S_f (s_i, \alpha^n)$ for all s_i and α^n, n = 1 2 3 $\cdots$. It is noted, in conclusion, that before the result of Theorem 3.5 can be applied to investigate ILF properties it is necessary first to test for the IL condition. There exist machines for which

$$\# \left\{ S_f (s, \alpha) \cap S_i (\beta^L) \right\} < 2$$

for every $s \in S$, $\alpha \in Y(s)$ and $\beta^L \in Y^L$ but are not INV #L if the IL condition is not satisfied. The machine of Figure 3.3 is an example which illustrates such behavior for L = 1.

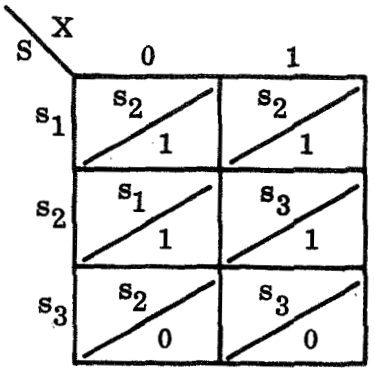


FIGURE 3.3 - A NON-IL FINITE STATE MACHINE

In this Chapter we have considered the concepts of information losslessness and of information losslessness of finite order. These concepts were related to our definitions of invertibility. A necessary and sufficient condition for a certain class of FSM's to be IL was presented and some bounds associated with the IL property were considered. In the next Chapter we will investigate the application of a particular state reduction procedure and its implications on FSM invertibility.

CHAPTER IV

ON THE STATE REDUCTION OF INVERTIBLE MACHINES

Two states, say s_i and s_j, are said to be n - equivalent if and only if $\lambda(s_i, x^n) = \lambda(s_j, x^n)$ for every x^n. Two states are equivalent if and only if they are n - equivalent for every $n \geq 0$. A finite state machine is said to be minimal if and only if there exist no two equivalent states in the state set. These are the usual concepts of state equivalence and minimal machines which have been treated extensively in the literature. In the study of information lossless and invertible machines some variations on these definitions of equivalence and minimality are possible and useful. These variations may permit state reduction of machines which are minimal in the usual sense at the outset. The resultant state reduced machine can be shown to be invertible if the original machine was invertible.

An extension of the state reduction procedure which preserves invertibility and in certain cases information losslessness is possible, in general, because of the independence between these characteristics and input sequences. In other words, the IL or INV #L characteristics of an FSM depend only on the output sequences which are possible from each state and not, in an essential way, on the input sequences which produce them. To formalize this assertion we state the following.

Lemma 4.1: An FSM M remains IL (INV #L) or remains not IL (INV #L) under any interchange of both next state and output entries between two designated columns in any row of the state transition table (see Figure 1.1 (b)) for M.

Proof: Consider the invertibility test graph or ITG (see Figure 3.2) for any machine, M. The chains of compatible state pairs on the ITG are determined entirely by the output labels and next state assignments contained in each row of the state transition table for M. The ITG does not depend on the input symbol for which the output label and next state are defined. It follows that the ITG's for any two N-state machines which have the same possible next state and output label entries in each row of their state transition tables are identical under any ordering of these entries. Since the machines yield the same ITG they possess the same IL and INV #L properties.

Because of this exclusive dependence on output labels it may be suspected that the usual definition of state equivalence is too restrictive if only inverse properties are to be retained in the state reduction of machines. If the state behavior and output response for particular input sequences are not of interest, then state "equivalence" may be based only on possible output sequences without regard for the input sequences which produced them.

The definition of state equivalence which seems to be of greatest usefulness in this respect is the following.

Definition 4.1: Two states, s_i and s_j, are n - output equivalent, written $s_i \, O_n \, s_j$, if $Y^n(s_i) = Y^n(s_j)$.

Thus two states are n - output equivalent if they allow precisely the same set of output sequences of length n.

Definition 4.2: Two states s_i and s_j are output equivalent, written $s_i \, O_\infty \, s_j$, if $s_i \, O_n \, s_j$ for every integer $n \geq 0$.

For example, in the two state, binary machine given in Figure 4.1 states s_1 and s_2 are output equivalent since $Y^n(s_1) = Y^n(s_2)$ for every n.

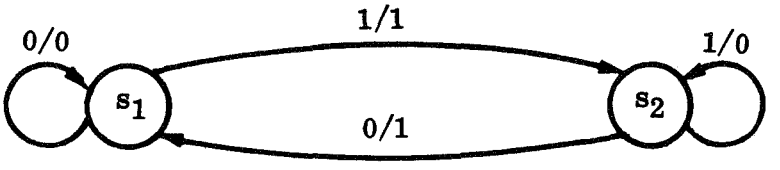


FIGURE 4.1 - A BINARY FSM WITH TWO OUTPUT EQUIVALENT STATES

From the definition of output minimal states we may characterize the corresponding minimal FSM by

Definition 4.3: An FSM is said to be output minimal if there exist no s_i and $s_j \in S$ such that $s_i \, O_\infty \, s_j$.

Clearly every output minimal machine is also minimal in the usual sense. It is obvious that the relation O_n is an equivalence relation on the state set S for every n. Consequently, O_n induces a partition of S. Every s_i and s_j satisfying $s_i \, O_n \, s_j$ are contained in the same equivalence class of π_n, the partition induced by O_n.

Many of the properties of state equivalence and partitions induced by the usual state equivalence relation carry over to the corresponding output equivalence and output equivalence induced partitions. For example, the uniqueness

of the partition π_n may be shown as for the partition induced by normal state n - equivalence. However, one important property is lost in the extension. It is not, in general, true that if $\pi_n = \pi_{n+1}$ for some n, then $\pi_{n+1} = \pi_{n+k}$ for every $k \geq 1$. This property holds for partitions induced by the usual state n - equivalence relation and is a key element in the proof that two states which are (N-1) - equivalent, where N = #S are n - equivalent for every n or are simply equivalent. The example machine of Figure 4.2 shows a five state binary machine for which $\pi_1 = \pi_2$ but $\pi_2 \neq \pi_3 \neq \pi_4 = \pi_\infty$.

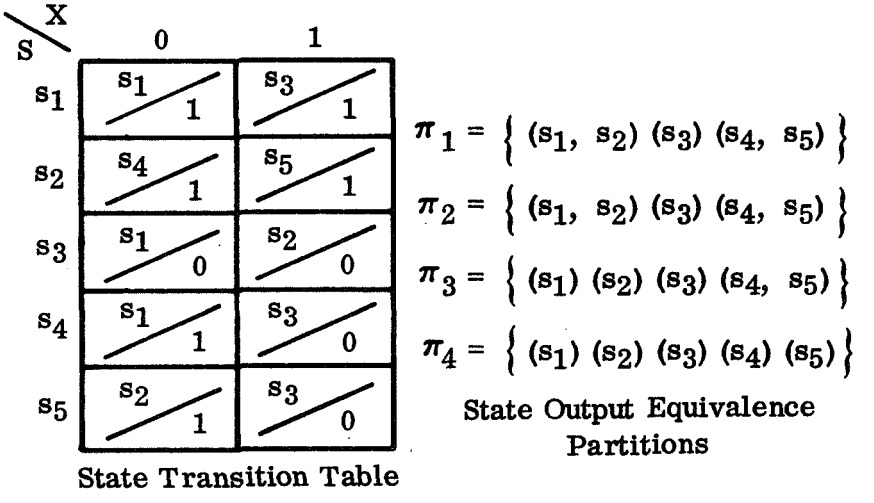


FIGURE 4.2 – A BINARY FSM AND CORRESPONDING OUTPUT EQUIVALENCE PARTITIONS

We note that $\pi_4 = \pi_{(N-1)} = \pi_\infty$ for the machine of Figure 4.2 even though $\pi_1 = \pi_2 \neq \pi_4$. This (i.e., $\pi_{N-1} = \pi_\infty$) appears to be a property of state output equivalence partitions as in the case of partitions induced by normal state equivalence. The proof has eluded us thus far, however. Actually, we have not been able to show any bound on the length of the test for output equivalence for arbitrary finite state machines.

In the special case for which a machine is INV #L, is strongly connected and has #X = #Y it is possible to show that the test for state output equivalence has finite length. In this case a bound on the maximum index i such that $\pi_i \neq \pi_\infty$ is a consequence of the following theorem.

Theorem 4.1: If M is an INV #L, strongly connected FSM and #X = #Y, then $\pi_L = \pi_\infty$.

Proof: Suppose $s_i \, O_L \, s_j$. Let α^L be any length L output sequence in $Y^L(s_i) = Y^L(s_j)$. By Theorem 2.3, given any $y^n \in Y^n$ for any n, it is possible to find states in $S_f(s_i, \alpha^L)$ and $S_f(s_j, \alpha^L)$ respectively which allow the sequence y^n. Hence, for any $n \geq 0$, $Y^{L+n}(s_i) = \left\{ \alpha^L y^n : \alpha^L \in Y^L(s_i) \text{ and } y^n \in Y^n \right\} = Y^{L+n}(s_j)$. By definition it follows that $s_i \, O_{L+n} \, s_j$. Since n is arbitrary we have $s_i \, O_\infty \, s_j$ and consequently $\pi_L = \pi_\infty$.

It can be shown (see Chapter VIII) that, for any invertible FSM, the inverse delay L is at most N(N-1)/2. It follows immediately that, for the class of machines considered, $\pi_{N(N-1)/2} = \pi_\infty$.

It has been shown that π_L is the final partition for an INV #L, strongly connected FSM for which #X = #Y. We note, however, that the minimum n for which $\pi_n = \pi_\infty$ does not, in general, define the inverse delay of an invertible machine. The binary, strongly connected, INV #4 machine of Figure 4.3 illustrates this point.

S \ X	0	1
s_1	s_1 / 0	s_5 / 0
s_2	s_1 / 0	s_6 / 0
s_3	s_2 / 0	s_7 / 0
s_4	s_3 / 1	s_5 / 1
s_5	s_4 / 0	s_8 / 0
s_6	s_4 / 0	s_8 / 1
s_7	s_4 / 0	s_9 / 0
s_8	s_4 / 1	s_8 / 1
s_9	s_4 / 1	s_8 / 0

State Transition Table

$\pi_1 = \{(s_1, s_2, s_3, s_5, s_7)(s_4, s_8)(s_6, s_9)\}$

$\pi_2 = \{(s_1, s_3)(s_2, s_7)(s_4)(s_5)(s_6, s_9)(s_8)\}$

$\pi_3 = \{(s_1, s_3)(s_2)(s_4)(s_5)(s_6)(s_7)(s_8)(s_9)\}$

$\pi_4 = \{(s_1, s_3)(s_2)(s_4)(s_5)(s_6)(s_7)(s_8)(s_9)\}$

State Output Equivalence Partitions

FIGURE 4.3 - AN INV #4 FSM WITH $\pi_3 = \pi_\infty$

By application of any of the tests for invertibility described in Chapter III it is possible to show that the machine of Figure 4.3 is INV #4. We observe, however that $\pi_3 = \pi_4$. By Theorem 4.1 we know that π_4 is the final partition and no further refinements are possible. It is seen that the final partition contains two output equivalent states, s_1 and s_3. These states are not equivalent in the usual sense, however. Consequently, the machine of Figure 4.3 is minimal in the usual sense and no state reduction by deletion of equivalent states is possible. It is natural, nevertheless, to investigate the properties of machines which result from state reduction of output equivalent states. As will be shown these resultant state reduced or output minimal machines are of particular interest when the original machine is invertible or information lossless.

To begin our investigation of the correspondence between the invertibility of a machine M and of its output minimal version(s) we first formally define an output minimal representation of M. To do this we make use of the following notation. Let $[s]$ be the block of π_{∞} containing s. In addition let $\{s_{j1}, s_{j2}, \cdots\cdots s_{jm}\}$ be any representative states, one from each of the m distinct blocks of π_{∞} for a machine $M = \langle S, X, Y, \delta, \lambda \rangle$.

Definition 4.4: An output minimal representation (OMR) of an FSM M is given by $M^{o}(s_{j1}, s_{j2}, \cdots\cdots s_{jm}) = \langle S^{o}, X, Y, \delta^{o}, \lambda^{o} \rangle$

where

$$S^{o} = \{ [s_{ji}] : i = 1, 2, \cdots\cdots m \}$$

$$\delta^{o}([s_{ji}], x) = [\delta(s_{ji}, x)]$$

$$\lambda^{o}([s_{ji}], x) = \lambda(s_{ji}, x) .$$

It is easily seen that an output minimal representation of a given machine need not be unique. In general, if $\#\pi_{\infty} < N$ there may be many non-isomorphic output minimal versions of the same machine. Every output minimal representation of a given machine has the same number (i.e. $\#\pi_{\infty} = m$) of states, however.

From the definition of an output minimal representation of a machine it is possible to show a somewhat evident but nonetheless important property of such state reduced machines. This property is given as

Lemma 4.2: If $M^{o}(s_{j1}, s_{j2}, \cdots\cdots s_{jm})$ is an OMR of an FSM M and if $s_k \in [s_{ji}]$ for some index i, then $Y^{n}(s_k) = Y^{n}([s_{ji}])$ for every n. $Y^{n}([s_{ji}])$ is taken to mean the set of output sequences of length n allowed by state $[s_{ji}] \in S^{o}$.

Proof: From the definition of output equivalent states it follows that $Y^n(s_k) = Y^n(s_{ji})$ for $s_k \in [s_{ji}]$. Hence, it is only necessary to show that $Y^n(s_{ji}) = Y^n([s_{ji}])$. Suppose that t is the least integer such that $Y^t(s_{ji}) \neq Y^t([s_{ji}])$ for any $[s_{ji}] \in S^o$. Clearly $t > 1$ since by Definition 4.4, $\lambda^o([s_{ji}], x) = \lambda(s_{ji}, x)$ for every $x \in X$. In addition, by our assumption that n is minimum we have $Y^{t-1}(\delta(s_{ji}, x)) = Y^{t-1}(\delta^o([s_{ji}], x))$ since $\delta^o([s_{ji}], x) = [\delta(s_{ji}, x)]$. But this implies that $Y^t(s_{ji}) = Y^t([s_{ji}])$, contrary to our assumption. Hence, for every $s_k \in [s_{ji}]$ and for every n we conclude that $Y^n(s_k) = Y^n([s_{ji}])$.

It is possible to show that many of the properties of finite state machines are preserved in their output minimal representations. In particular, in the case of invertible machines we can show the following relation.

Theorem 4.2: Let M be any FSM and let $M^o(s_{j1}, s_{j2} \cdots s_{jm})$ be any OMR of M, then $M^o(s_{j1}, s_{j2}, \cdots s_{jm})$ is INV #L' for some $L' \leq L$ if M is INV #L. Further, if M is INV #L, then there exists at least one OMR of M such that $M^o(s_{j1}, s_{j2}, \cdots s_{jm})$ is INV #L.

Proof: Let M be an INV #L machine and let $M^o(s_{j1}, s_{j2}, \cdots\cdots s_{jm})$ be any OMR of M. Suppose $M^o(s_{j1}, s_{j2}, \cdots s_{jm})$ is not INV #L' for any $L' \leq L$. It follows that there exists $[s_{ji}] \in S^o$ and input sequences $a^{L+1} = a_1 a_2 \cdots a_{L+1}$ and $b^{L+1} = b_1 b_2 \cdots b_{L+1}$ with $a_1 \neq b_1$ such that $\lambda^o([s_{ji}], a^{L+1}) = \lambda^o([s_{ji}], b^{L+1})$. By Definition 4.4 $\lambda(s_{ji}, a_1) = \lambda(s_{ji}, b_1)$ and also $\delta^o([s_{ji}], a_1) = [\delta(s_{ji}, a_1)]$ and $\delta^o([s_{ji}], b_1) = [\delta(s_{ji}, b_1)]$.

Consequently, both $\delta(s_{ji}, a_1)$ and $\delta(s_{ji}, b_1)$ allow a common output sequence of length L. It follows that M is not INV #L, contrary to our hypothesis. Hence, if M is INV #L then any OMR of M is INV #L' for some $L' \leq L$.

It remains to show that at least one OMR of M is INV #L. If M is INV #L there exists $s_k \in S$ and input sequences $c^L = c_1\ c_2 \cdots c_L$ and $d^L = d_1\ d_2 \cdots d_L$ with $c_1 \neq d_1$ such that $\lambda(s_k, c^L) = \lambda(s_k, d^L)$. Define $M^o(s_{j1}, s_{j2}, \cdots s_{jm})$ such that $s_{ji} = s_k$ for some i. By definition 4.4 it follows that $\lambda^o(\lceil s_{ji} \rceil, c_1) = \lambda^o(\lceil s_{ji} \rceil, d_1)$ and in addition that $\delta^o(\lceil s_{ji} \rceil, c_1) = \lceil \delta(s_k, c_1) \rceil$ and $\delta^o(\lceil s_{ji} \rceil, d_1) = \lceil \delta(s_k, d_1) \rceil$. Consequently, both $\delta^o(\lceil s_{ji} \rceil, c_1)$ and $\delta^o(\lceil s_{ji} \rceil, d_1)$ allow a common output sequence of length L-1. Hence, $M^o(s_{ji}, s_{j2}, \cdots s_{jm})$ is not INV #L' for $L' < L$. Clearly, from the initial result of the theorem, $M^o(s_{j1}, s_{j2}, \cdots s_{jm})$ is INV #L and the proof of the theorem is completed.

To show the existence of an invertible machine which has more than one output minimal representation with dissimilar inverse delays, consider the machine of Figure 4.3. Two possible state reduced or output minimal versions of this machine corresponding to the two choices of representatives s_i from the class (s_1, s_3) are possible. The two output minimal representations are shown in Figure 4.4.

It may be shown that $M^o(s_3, s_2, s_4, s_5, s_6, s_7, s_8, s_9)$ is INV #4 and hence retains the inverse delay of the original machine. Machine $M^o(s_1, s_2, s_4, s_5, s_6, s_7, s_8, s_9)$, on the other hand is INV #2 and, in addition, is not

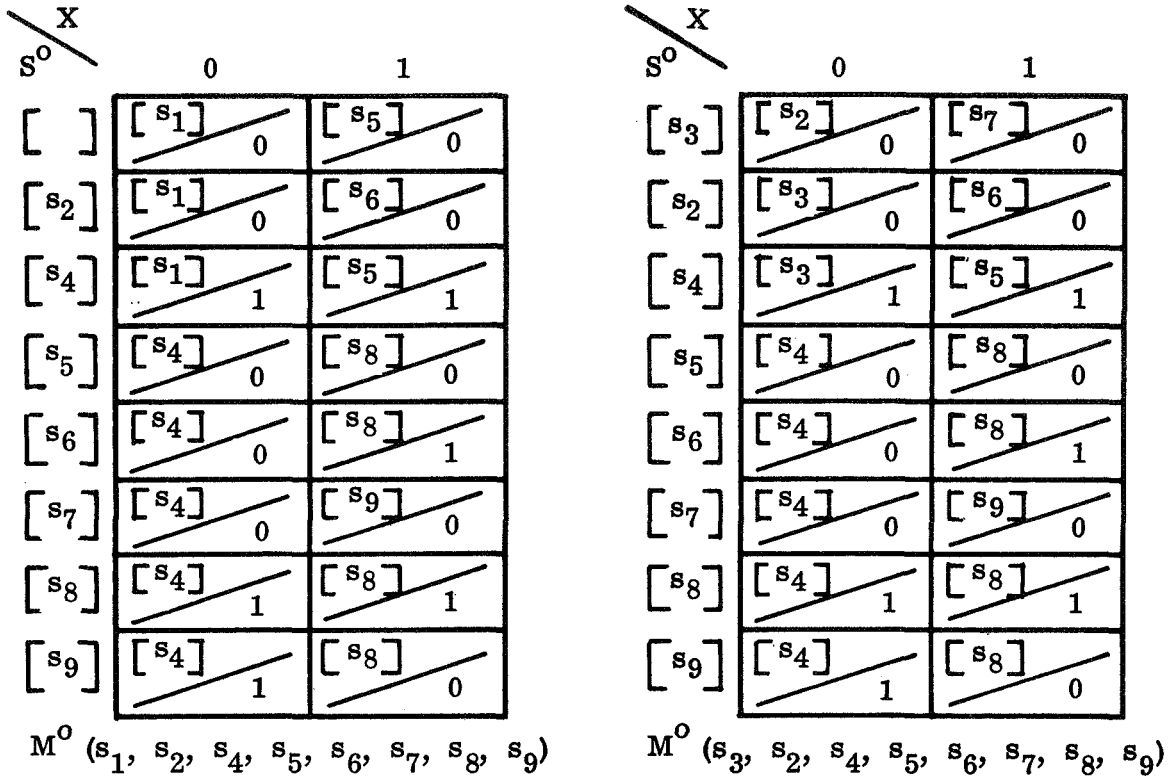


FIGURE 4.4 - TWO OUTPUT MINIMAL REPRESENTATIONS OF THE FSM OF FIGURE 4.3

strongly connected unlike the original machine and the alternate output minimal representation. States $[s_2]$, $[s_6]$, $[s_7]$ and $[s_9]$ of M^o (s_1, s_2, s_4, s_5, s_6, s_7, s_8, s_9) are transient states while the remaining states form a strongly connected INV #2 submachine.

Although it is not possible to show that the IL property is preserved by state reduction of output equivalent states for the general class of finite state machines[1], it is possible to show that IL behavior is preserved for an important class of machines, i.e., strongly connected machines. To aid in the proof of this result we will use the following lemma.

[1]It should be noted also that, for general FSM's, IL behavior may be lost by state reduction of states which are equivalent in the usual sense.

Lemma 4.3: Let M be an IL, strongly connected FSM and let n be any positive integer. Then, for any $s_i \in S$ and $\alpha^n \in Y^n(s_i)$, there can exist no two output equivalent states in $S_f(s_i, \alpha^n)$.

Proof: Suppose for some FSM M there exists s_j and $s_k \in S_f(s_i, \alpha^n)$ for some s_i and $\alpha^n \in Y^n(s_i)$ such that $s_j \, O_\infty \, s_k$. Suppose further that M is strongly connected. Let x^t be any input sequence such that $\delta(s_j, x^t) = s_i$ and let $\lambda(s_j, x^t) = \beta^t$. Clearly $s_i \in S_i((\alpha^n \beta^t)^m)$ for every m. Suppose $\#S_f(s_i, (\alpha^n \beta^t)^m) \leq \#S_f(s_i, (\alpha^n \beta^t)^{m-1})$ for some m. This implies that $(\beta^t \alpha^n)^m$ is allowed by s_j but not by s_k and consequently that $s_j \notin [s_k]$ which is a contradiction. Hence $\#S_f(s_i, (\alpha^n \beta^t)^m) > \#S_f(s_i, (\alpha^n \beta^t)^{m-1})$ for every m. It follows that for some m', $\#S_f(s_i, (\alpha^n \beta^t)^{m'}) = N = \#S$ and for $m'+1$ we must have $\#X^{nt(m'+1)}(s_i, (\alpha^n \beta^t)^{m'+1}) > \#S_f(s_i (\alpha^n \beta^t)^{m'+1})$. Hence, M is not IL and the lemma follows.

With the aid of Lemma 4.3 we may state the following.

Theorem 4.3: If M is a strongly connected and IL FSM, then every OMR of M is also IL.

Proof: Let $M^o(s_{j1}, s_{j2}, \cdots s_{jm})$ be an OMR of a strongly connected, IL machine M. Suppose $M^o(s_{j1}, s_{j2}, \cdots\cdots s_{jm})$ is not IL. It follows that there exist $[s_{ji}] \in S^o$ and input sequences $x^n = x_1 x_2 \cdots x_n$ and $u^n = u_1 u_2 \cdots\cdots u_n$ with $x_1 \neq u_1$ such that $\lambda^o([s_{ji}], x^n) = \lambda^o([s_{ji}], u^n) = \alpha^n$ and $\delta^o([s_{ji}], x^n) = \delta^o([s_{ji}], u^n)$. But this implies that $S_f(s_{ji}, \alpha^n)$ contains two output equivalent states and by Lemma 4.3 M is not IL. Hence, if M is IL, then every OMR of M is also IL.

To show that the strongly connected restriction of Theorem 4.3 is necessary we give an example of an IL machine which is not strongly connected and which has an output minimal representation that is not IL. The machine of Figure 4.5 (a) is such an example.

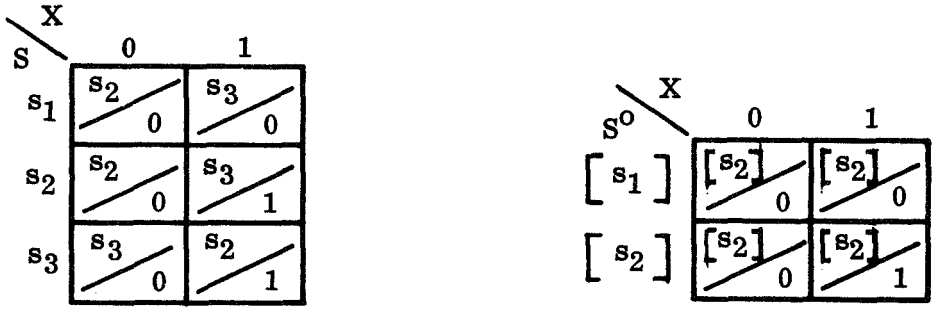


FIGURE 4.5 - AN IL, NON-STRONGLY CONNECTED FSM M AND A NON-IL OUTPUT MINIMAL REPRESENTATION OF M

It is possible to show several other structure preserving properties of output minimal representations of certain classes of invertible machines. In the case of strongly connected machines whose input and output sets have the same order, it can be shown that the order of final state sets is preserved for output sequences of all lengths. To prove this assertion we make use of the following lemma.

Lemma 4.4: If M is an INV #L, strongly connected FSM and #X = #Y = q, then for every s_i and $s_j \in S$ such that $s_i \in [s_j]$ we have $\#S_f(s_i, \alpha^n) = \#S_f(s_j, \alpha^n)$ for every n and for every $\alpha^n \in Y^n$.

Proof: For $n \geq L$ we have $\#S_f(s_i, \alpha^n) = \#S_f, (s_j, \alpha^n)$ by Theorem 2.1. Suppose $n < L$. Define the set of output sequences

$$Y^m(S_f(s_i, \alpha^n)) = \left\{ \bigcup_{s_k \in S_f(s_i, \alpha^n)} Y^m(s_k) \right\}.$$

If $s_i \in [s_j]$, it follows from Lemma 4.2 that $Y^m(S_f(s_i, \alpha^n)) = Y^m(S_f(s_j, \alpha^n))$ for every m. Let m = L-n. Since $\#S_f(s_i, \alpha^n \gamma^{L-n}) = \#S_f(s_j \alpha^n \gamma^{L-n})$ for every output sequence γ^{L-n}, it is clear that

$$\sum_{s_q \in S_f(s_i, \alpha^n)} \#X^{L-n}(s_q, \gamma^{L-n}) = \sum_{s_p \in S_f(s_j, \alpha^n)} \#X^{L-n}(s_p, \gamma^{L-n}) .$$

In addition, we may write

$$\left[\#Y^{L-n}(S_f(s_i, \alpha^n))\right] \cdot \left[\sum_{s_q \in S_f(s_i, \alpha^n)} \#X^{L-n}(s_q, \gamma^{L-n})\right] = q^{L-n} \cdot \left[\#S_f(s_i, \alpha^n)\right]$$

and

$$\left[\#Y^{L-n}(S_f(s_j, \alpha^n))\right] \cdot \left[\sum_{s_p \in S_f(s_j, \alpha^n)} \#X^{L-n}(s_p, \gamma^{L-n})\right] = q^{L-n} \cdot \left[\#S_f(s_j, \alpha^n)\right].$$

Hence, $\#S_f(s_i, \alpha^n) = \#S_f(s_j, \alpha^n)$ for every n and the lemma is proved.

With the aid of Lemma 4.4 it is possible to assert the following.

Theorem 4.4: If M is a strongly connected, INV #L FSM with #X = #Y and $M^o(s_{j1}, s_{j2} \cdots s_{jm})$ is an OMR of M, then for every n, for every s_{ji} and for every $s_k \in [s_{ji}]$, $\#S_f(s_k, \alpha^n) = \#S_f([s_{ji}], \alpha^n)$.

Proof: As a result of Lemma 4.4 it is only necessary to show that $\#S_f(s_{ji}, \alpha^n) = \#S_f([s_{ji}], \alpha^n)$. Since by Definition 4.4, $\lambda^o([s_{ji}], x) = \lambda(s_{ji}, x)$ and since $M^o(s_{j1}, s_{j2}, \cdots s_{jm})$ is invertible by Theorem 4.2, we have $\#X([s_{ji}], \alpha) = \#X(s_{ji}, \alpha) = \#S_f([s_{ji}], \alpha) = \#S_f(s_{ji}, \alpha)$ for every $\alpha \in Y(s_{ji})$. Hence, the theorem holds for n = 1. Suppose $t > 1$ is the least integer such that for any $[s_{ji}] \in S^o$, $\#S_f([s_{ji}], \beta^t) \neq \#S_f(s_{ji}, \beta^t)$. But we may write

$$\#S_f\left(\left[s_{ji}\right]\beta^t\right) = \sum_{x_i \in X\left(\left[s_{ji}\right],\ \beta_1\right)} \#S_f\left(\delta^o\left(\left[s_{ji}\right],\ x_i\right),\ \beta_2\ \beta_3 \cdots\ \beta_t\right)$$

and

$$\#S_f\left(s_{ji},\ \beta^t\right) = \sum_{x_i \in X\left(s_{ji},\ \beta_1\right)} \#S_f\left(\delta(s_{ji},\ x_i),\ \beta_2\ \beta_3 \cdots\ \beta_t\right)$$

where $\beta^t = \beta_1\ \beta_2 \cdots\ \beta_t$. By our hypothesis that t is minimum we have $\#S_f\left(\delta^o\left(\left[s_{ji}\right],\ x_i\right),\ \beta_2\ \beta_3 \cdots\ \beta_t\right) = \#S_f\left(\delta(s_{ji},\ x_i),\ \beta_2\ \beta_3 \cdots\ \beta_t\right)$. Since $X\left(\left[s_{ji}\right],\ \beta_1\right) = X\left(s_{ji},\ \beta_1\right)$, it follows that $\#S_f\left(\left[s_{ji}\right],\ \beta^t\right) = \#S_f\left(s_{ji},\ \beta^t\right)$; contrary to our assumption. Hence, by contradiction, the theorem is proved.

From Theorem 4.4 it follows that the state reduced machine has the same maximum final state set order as the original machine if the original machine satisfies the condition of the theorem. Since a strongly connected, INV #L machine for which $\#X = \#Y = q$, for q a prime, satisfies $L \geq j$, where q^j is the maximum final state set order, it is clear in this case that L', the inverse delay of the state reduced OMR, is bounded by

$$j \leq L' \leq L\ .$$

Another relation of some interest concerning the properties of certain invertible machines and their output minimal representations can be given as

Theorem 4.5: Let $M^o\left(s_{j1},\ s_{j2},\ \cdots\ s_{jm}\right)$ be an output minimal representation of a strongly connected, INV #L FSM M with #X = #Y. If $M^o\left(s_{j1},\ s_{j2},\ \cdots\ s_{jm}\right)$ is INV #L' for $L' < L$, then $M^o\left(s_{j1},\ s_{j2},\ \cdots\ s_{jm}\right)$ is not strongly connected.

Proof: By Theorem 4.2 we know that every OMR of an INV #L machine M is INV #L' for some $L' \leq L$. Suppose M is strongly connected and #X = #Y. Let

M^o $(s_{j1}, s_{j2} \cdots s_{jm})$ be a strongly connected OMR of M with inverse delay $L' < L$. It follows that for every $[s_{ji}]$ and every $\alpha^n \in Y^n$ ($[s_{ji}]$) where $n \geq L'$ that $\#S_f$ ($[s_{ji}]$, α^n) = J for some J as a result of Theorem 2.1. But by Theorem 4.4 $\#S_f$ $(s_k, \alpha^n) = \#S_f$ ($[s_{ji}]$, α^n) for every $s_k \in [s_{ji}]$. Hence, $\#S_f$ (s_{ji}, α^n) = J for every $n \geq L'$. However, since M is INV #L, there exists some $s_k \in S$ and $a^L = a_1\ a_2 \cdots\cdots a_L$ and $b^L = b_1\ b_2 \cdots b_L$ with $a_1 \neq b_1$ such that $\lambda(s_k, a^L) = \lambda(s_k, b^L) = \beta^L = \beta_1\ \beta_2 \cdots\cdots \beta_L$. But this implies that $\#S_f$ $(\delta(s_k, a_1), \beta_2\ \beta_3 \cdots\cdots \beta_L) < J$ and $\#S_f(\delta(s_k, b_1), \beta_2\ \beta_3 \cdots \beta_L) < J$. Since $L-1 \geq L'$ and since $\delta(s_k, a_1)$ and $\delta(s_k, b_1)$ each belong to some equivalence class of π_∞, we have a contradiction of Theorem 4.4. Consequently, if $L' < L$, then M^o $(s_{j1}, s_{j2}, \cdots\cdots s_{jm})$ is not strongly connected.

In this chapter we have introduced a procedure for state reduction which is of particular interest when applied to invertible machines. It is seen that output minimal representations preserve the invertibility and in certain cases the information losslessness of the original machine. Consequently, in some applications, as possibly in the design of encoders and decoders for discrete information channels (where it is not important which input sequence produces a particular output sequence), the described state reduction procedure may be usefully applied. The resultant machine or output minimal representation will yield the same possible output sequences as the original machine and will be invertible if the original machine is invertible. Furthermore, there exists a particular state correspondence such that the resultant reduced machine has the same inverse delay as the original machine. State reduction based on the

concept of output equivalence with the results described is possible because IL and INV #L properties of a finite state machine depend only on state and output sequences and not, in an essential way, on the input sequences which produced them.

CHAPTER V

FINITE INPUT MEMORY MACHINES

In this chapter we will consider the invertibility and information losslessness of finite input memory machines.

Definition 5.1: An FSM M has finite input memory μ(FIM (μ)) if (μ) is the least integer such that the output at time t can be expressed in the form

$$y(t) = f(x(t), x(t-1), \cdots\cdots\cdots x(t-\mu))$$

for $t \geq \mu$. If no such μ exists, M is said to have infinite input memory.

The concept of memory can be generalized to both input/output memory as well as to output memory alone. The memory characteristics of finite state machines have been studied extensively by several investigators (see Vairavan[1] and the bibliography presented therein).

For our purposes we will consider only non-degenerate, FIM (μ) machines. The following definition is due to Vairavan.

Definition 5.2: An FSM $M = \langle S, X, Y, \delta, \lambda \rangle$ is non-degenerate if the mapping, $\delta: S \times X \longrightarrow S$, is onto.

In canonical realization form, non-degenerate FIM (μ) machines are composed of a shift register and combinatorial logic as shown in Figure 5.1.

[1]K. Vairavan, "On the Memory of Finite State Machines", Technical Report No. EE-683, University of Notre Dame, Department of Electrical Eng., April 7, 1968.

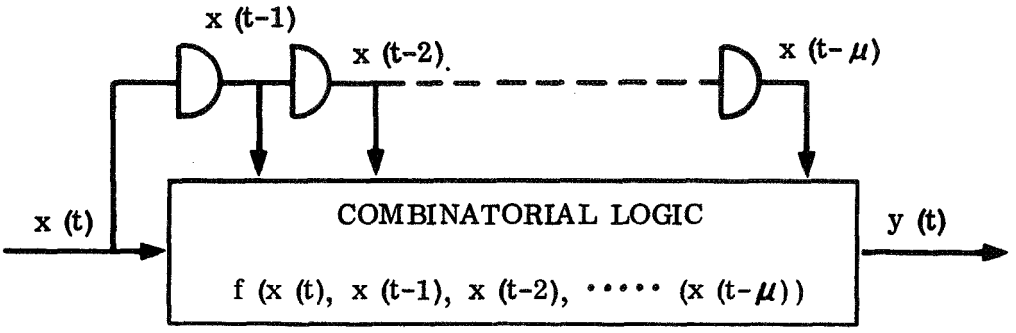


FIGURE 5.1 - CANONICAL REALIZATION OF A NON-DEGENERATE, FIM (μ) FINITE STATE MACHINE

The realization of Figure 5.1 is one in which any non-degenerate, FIM (μ) machine may be synthesized. Vairavan has shown that all non-degenerate, FIM (μ) machines have a unique output function f and that any two such machines which are non-degenerate and have the same output function are equivalent. Since our restriction to non-degenerate machines excludes only those machines which have transient states we lose little generality in limiting our attention to FIM (μ) machines which may be synthesized in the form of Figure 5.1. In the work which follows we will consider only FIM (μ) machines which are in the canonical form of Figure 5.1.

We observe that X^{μ}, the set of all input sequences of length μ, is an appropriate choice for the state set of machines in the canonical form of Figure 5.1. Hence, if #X = q, every such machine has precisely q^{μ} states. Further, it has been shown by Vairavan that q^{μ} is an upper bound on the order of the state set for non-degenerate, minimal, FIM (μ) machines. It is also clear that in canonical form, non-degenerate, FIM (μ) machines are completely defined by the function f which yields the present output. The next state is defined by the present input and the preceding $\mu - 1$ input letters. It follows that all such machines are strongly connected.

We begin our investigation of the invertibility of non-degenerate, FIM (μ) machines with the following result concerning the order of the initial state sets for output sequences of length L or longer.

Theorem 5.1: If M is a non-degenerate, FIM (μ), INV #L FSM with #X = #Y = q and q^{μ} states, then there exists some K such that $\#S_i(y^n) = K$ for every y^n with $n \geq L$.

Proof: Let m be the least integer such that $m\mu \geq L$. By Theorem 2.2, $\#Y^{m\mu}(s_i) = q^{m\mu}/J$ for some J and for every $s_i \in S$. Moreover, since M is INV #L, it is clear that for every $n \geq L$ and for every $y^n \in Y^n$, there exists one and only one state $s_j \in S_f(s_i, \alpha^{m\mu})$ for every $s_i \in S$ and $\alpha^{m\mu} \in Y^{m\mu}(s_i)$ such that $s_j \in S_i(y^n)$. But from any initial state each of the q^{μ} states in the state set S occurs precisely $q^{(m-1)\mu}$ times as a final state for input sequences of length $m\mu$. Hence, it follows that $\#S_i(y^n) = \#Y^{m\mu}(s_i) / q^{(m-1)\mu} = q^{\mu}/J$. Consequently, if $K = q^{\mu}/J$, the assertion of the theorem is proved.

We remark that the assertion of Theorem 5.1 is not true in general for invertible FSM's but results from the particular state transition structure of the class of machines considered as well as from the INV #L condition. As a consequence of Theorem 5.1 we may show an additional property of such machines.

Theorem 5.2: If M is a non-degenerate, FIM (μ), INV #L FSM with #X = #Y = q and q^{μ} states, then

$$\sum_{s_i \in S} \#X^n(s_i, y^n) = q^{\mu}$$

for every $n \geq 1$ and for every $y^n \in Y^n$.

Proof: For $n \geq L$ the assertion of the theorem follows immediately. In this case we have $\#X^n(s_i, \alpha^n) = \#X^n(s_i, \beta^n) = J$ for every s_i and for every α^n and $\beta^n \in Y^n(s_i)$ by Theorem 2.1. In addition, by Theorem 5.1, we have $\#S_i(\alpha^n) = \#S_i(\beta^n) = q^\mu/J$. Hence, for any $y^n \in Y^n$ with $n \geq L$ it follows that

$$\sum_{s_i \in S} \#X^n(s_i, y^n) = q^\mu \quad .$$

Consider the case for which $n < L$. Suppose for some α^n with $n < L$ we have

$$\sum_{s_i \in S} \#X^n(s_i, \alpha^n) > q^\mu \quad .$$

Since $\#X = \#Y = q$, it follows that there exists β^n such that

$$\sum_{s_i \in S} \#X^n(s_i, \beta^n) < q^\mu$$

and consequently such that

$$\sum_{s_i \in S} \#X^n(s_i, \alpha^n) > \sum_{s_i \in S} \#X^n(s_i, \beta^n) \quad .$$

This means that over the state set S more length n input sequences are mapped into the output sequence α^n than into the sequence β^n. But, if we consider the pairs of distinct initial states and length mn input sequences (s_j, x^{mn}) for any $m \geq 1$, we note that since M is a non-degenerate, FIM (μ) FSM with q^μ states, each state in S satisfies $\delta(s_j, x^{mn})$ precisely q^{mn} times for distinct pairs (s_j, x^{mn}). Hence, there exist precisely q^{mn} distinct pairs which may be associated with each state in the state set. It follows that the number of distinct pairs $(s_j, x^{(m+1)n})$ which correspond to length $(m+1)n$ output sequences whose last n digits define the sequences α^n and β^n are

$$q^{mn} \sum_{s_i \in S} \#X^n(s_i, \alpha^n) \text{ and } q^{mn} \sum_{s_i \in S} \#X^n(s_i, \beta^n)$$

respectively. But if

$$\sum_{s_i \in S} \#X^n (s_i, \alpha^n) > \sum_{s_i \in S} \#X^n (s_i, \beta^n) ,$$

it is always possible to find some length mn output sequence, say γ^{mn}, with $mn \geq L$ such that

$$\sum_{s_i \in S} \#X^{(m+1)n} (s_i, \gamma^{mn} \alpha^n) > \sum_{s_i \in S} \#X^{(m+1)n} (s_i, \gamma^{mn} \beta^n).$$

Consequently, we have a contradiction of our initial result for $n \geq L$ and we conclude that the theorem holds for every $n \geq 1$.

Theorem 5.2 has an interesting corollary in the case of binary machines. In this case it follows that

Corollary 5.2.1: If M is a binary, non-degenerate, FIM (μ), INV #L FSM with output function

$$y(t) = f(x(t), x(t-1), \cdots\cdots x(t-\mu)) ,$$

then there are precisely 2^{μ} terms in the canonical sum of products expansion of f.

Proof: By Theorem 5.2 it follows that $\sum_{s_i \in S} \#X (s_i, 0) = \sum_{s_i \in S} \#X (s_i, 1) = 2^{\mu}$. But this is entirely equivalent to the assertion of the corollary since each choice of x (t), x (t-1), $\cdots\cdots$ x ($t-\mu$) such that y (t) = 1 corresponds to a distinct term in the canonical sum of products expansion for f.

It is not true, however, that every binary FIM machine with 2^{μ} terms in the canonical sum of products expansion for f is invertible or even information

lossless. The non-degenerate, binary, FIM (2) machine with output function[2]

$$y(t) = x(t-1) \oplus (x(t) \cdot x(t-2))$$

is an example of such a machine which is not IL.

It is natural at this point to investigate constraints imposed on the output function of an FIM (μ) FSM in order to satisfy the invertibility condition. For small orders of L these constraints may be easily obtained. In the case of binary machines which are INV #0 it is well known (see Preparata[3]) that

Theorem 5.3: A binary, non-degenerate, FIM (μ), FSM is INV #0 if and only if it has an output function of the form

$$y(t) = x(t) \oplus g(x(t-1), x(t-2), \cdots\cdots x(t-\mu)) \ .$$

A similar result can be obtained in the case of INV #1 machines. In this case we have

Theorem 5.4: A binary, non-degenerate, FIM (μ) FSM M is INV #1 if and only if it has an output function of the form

$$y(t) = x(t-1) \oplus g(x(t-2), x(t-3), \cdots\cdots x(t-\mu)) \ .$$

Proof: The sufficiency of the condition for the INV #1 property is evident by inspection. To prove necessity we first show that if M is INV #1, then y (t) does not depend on x (t) or that the output function for M can be written in the form

$$y(t) = f(x(t-1), x(t-2), \cdots\cdots x(t-\mu)) \ .$$

[2]In this and succeeding chapters we will use the symbols $\oplus$, +, $\cdot$, and - for the Boolean operations of exclusive or, inclusive or, logical product and complementation respectively.

[3]F. Preparata, "Convolutional Transformations of Binary Sequences: Boolean Functions and Their Resynchronizing Properties", IEEE Transactions on Electronic Computers, Vol. EC-15, December 1966, pp. 898-908.

Suppose, to the contrary, that y (t) does depend on x (t). It follows that there exists a state, s_i, such that $\lambda(s_i, 0) \neq \lambda(s_i, 1)$. We note that any predecessor, say s_j, of s_i must also satisfy $\lambda(s_j, 0) \neq \lambda(s_j, 1)$. If not, then there exists a chain of compatible pairs on the invertibility test graph for M of length at least two and M is not INV #1. Since M is non-degenerate, a continuation of the above procedure for all possible predecessors of s_i, of s_j and of all predecessors of s_j, etc., will eventually exhaust the state set. At this point we will reach the conclusion that every state s satisfies $\lambda(s, 0) \neq \lambda(s, 1)$. But this requires that M is INV #0, contrary to our hypothesis. Hence, if M is INV #1, then y (t) does not depend on x (t).

We now must show that the output function f can be written in the form

$$y(t) = x(t-1) \oplus g(x(t-2), x(t-3), \cdots x(t-\mu)) .$$

Suppose no such function g exists. It follows that there exists a sequence of input digits $a_2\ a_3 \cdots\cdots a_\mu$ of length $\mu - 1$ such that if $x(t-2)\ x(t-3) \cdots x(t-\mu) = a_2\ a_3 \cdots a_\mu$, then $f(0, a_2, a_3, \cdots a_\mu) = f(1, a_2, a_3, \cdots a_\mu) = f(x(t-1), x(t-2), \cdots x(t-\mu))$. But the states $(0, a_2, a_3, \cdots a_\mu)$ and $(1, a_2, a_3, \cdots a_\mu)$ form a compatible pair on the invertibility test graph for M. Consequently, there must exist a compatible pair chain of length at least two and M is not INV #1. Hence, if M is INV #1, then f can be written in the specified form. This completes the proof of Theorem 5.4.

The necessity that x (t-L) appear in a modulo-two sum with some function of past inputs for a non-degenerate FIM machine to be INV #L in the case of L = 0 and L = 1 might lead to the conclusion that this is a necessary condition

for $L > 1$ also. This, however, is not the case. The machine whose sequential function is

$$y(t) = x(t-1) \oplus (x(t) \cdot x(t-2) \cdot \overline{x(t-3)})$$

is a counter-example to this conjecture. This counter-example is due to Prof. R. G. Gallager[4] of M.I.T. To show that the machine with the above output function is INV #2 consider the equations

$$y(t) = x(t-1) \oplus (x(t) \cdot x(t-2) \cdot \overline{x(t-3)})$$

$$y(t-1) = x(t-2) \oplus (x(t-1) \cdot x(t-3) \cdot \overline{x(t-4)}) \quad .$$

Solve the first equation for $x(t-1)$ and substitute for $x(t-1)$ in the second to obtain

$$y(t-1) = x(t-2) \oplus (y(t) \cdot x(t-3) \cdot \overline{x(t-4)}) \quad .$$

Clearly we may express $x(t-2)$ as a function of present and past output and past input digits. Therefore, a delay two inverse exists and the machine is INV #2.

We wish to extend the results of Theorems 5.3 and 5.4 to derive requirements on the form of the output function in order that a binary, non-degenerate, FIM (μ) machine be invertible. Unfortunately, we are not able to give both necessary and sufficient conditions for invertibility. However, we are able to define sufficient conditions; conditions which include a large class of invertible, FIM (μ) machines. A generalization of the form of the output function for the INV #2 FSM just described leads to the following result.

[4]Private Communication, Prof. R. G. Gallager to Prof. J. L. Massey, April 1967.

Theorem 5.5: A binary, non-degenerate, FIM (μ) FSM M is invertible if the following two conditions hold. (1) There exists an integer $k \leq \mu$ such that the output function for M can be written $y(t) = x(t-k) \oplus g(x(t), x(t-1), \cdots x(t-k+1), x(t-k-1), \cdots x(t-\mu))$ for some function g of μ variables. (2) For each $x(t-j)$; $0 \leq j \leq k-1$; that is non-idle in g there exists a distinct pair of unordered, non-idle variables $x(t-p_j)$ and $x(t-q_j)$ such that $\mu \geq p_j \geq 2k - j+1$ and $q_j = p_j - k+j$ and such that for each j every minterm in the canonical sum of products expansion of g contains the product of literals, $x(t-p_j) \cdot \overline{x(t-q_j)}$, or every minterm contains $\overline{x(t-p_j)} \cdot x(t-q_j)$.

Proof: The arguments required to show the validity of the theorem are unrewardingly tedious and hence, are omitted.

Binary, non-degenerate, FIM (μ) FSM's with output functions satisfying the conditions of Theorem 5.5 are INV #L for $L = 2k-n$ where n is the least integer j; $0 \leq j \leq k-1$; such that $x(t-j)$ is a non-idle variable in the output function. If all such $x(t-j)$ are idle variables, then $n = k$ and $L = k$. It is interesting to note that the formulation of Theorem 5.5 retains a characteristic noted for INV #1 machines. As a consequence of Theorem 5.4 it was observed that all binary, non-degenerate, FIM machines which are INV #1 have an output function f such that $x(t)$ is an idle variable in f. This same characteristic holds for the machines with inverse delay $L < 2k$ defined in accordance with Theorem 5.5. If the inverse delay L is odd then $x(t)$ must be an idle variable in f.

The formulation of Theorem 5.5 is not a canonical form for all binary, non-degenerate, invertible FIM machines. An output function which does not conform to the precise requirements of Theorem 5.5 but which may be taken to define an INV #2, non-degenerate, FIM (3) machine is given by

$$y\ (t) = x\ (t-1) \oplus (x\ (t) \cdot x\ (t-2) \cdot \overline{x\ (t-3)} + x\ (t-3))\ .$$

Necessary conditions on the output function f to insure invertibility of the corresponding FSM have not as yet been determined.

Another question of some interest concerns requirements on the output function of an FIM machine in order that the machine be information lossless. As in the case of conditions for invertibility we are unable to give both necessary and sufficient conditions for the output function of a binary, non-degenerate, FIM (μ) FSM to be representative of the information lossless property. We are, however, able to define some sufficient conditions for losslessness. First we observe that some of these conditions have already been given by Theorem 5.5 since every invertible machine is IL. Hence, we direct our attention in what follows to the class of information lossless but not invertible FIM machines.

To indicate the nature of the conditions to be considered as sufficient for IL behavior we give several examples of output functions which may be taken to define FIM, IL machines. First consider any non-degenerate, FIM (μ), FSM whose output function may be written in the form

$$y\ (t) = x\ (t-\mu) \oplus g\ (x\ (t),\ x\ (t-1),\ \cdots\ x\ (t-\mu+1))\ .$$

Clearly this machine is IL since we may solve for $x\ (t-\mu)$ explicity in terms

of present output y (t) and the present and μ-1 past input digits x (t), x (t-1), $\cdots\cdot$ x (t-μ+1) which are known if the final state is specified. With x (t-μ) so determined we may obtain x (t-μ-1) from y (t-1) and x (t-1), x (t-2), $\cdots\cdot$ x (t-μ). It is seen that all input digits x (t-μ-i); i $\geq$ 0; may be recovered in this manner.

Another more interesting example is the output function

$$y\ (t) = x\ (t-2) \oplus \overline{(x\ (t) \cdot x\ (t-1) \cdot x\ (t-3))} \ .$$

To show that the non-degenerate, FIM (3) machine corresponding to this output function is IL we write the expression for y (t-1);

$$y\ (t-1) = x\ (t-3) \oplus \overline{(x\ (t-1) \cdot x\ (t-2) \cdot (t-4))} \ .$$

Solve for x (t-3) and substitute in the first equation to obtain

$$y\ (t) = x\ (t-2) \oplus \overline{(x\ (t) \cdot x\ (t-1) \cdot y\ (t-1))}$$

which yields

$$x\ (t-3) = y\ (t-1) \oplus \overline{(x\ (t-1) \cdot x\ (t-2) \cdot y\ (t-2))} \ .$$

Since the final state is equivalent to (x (t), x (t-1), x (t-2)), knowledge of the final state allows the determination of x (t-3). A continuation of this procedure yields all prior input digits. It follows that the machine is IL.

The form of this last example leads to the following generalization.

Theorem 5.6: A binary, non-degenerate, FIM (μ) FSM M is IL but is not invertible if the following two conditions hold. (1) There exists an integer k $< \mu$ such that the output function for M can be written y (t) = x (t-k) $\oplus$ g (x (t), x (t-1), $\cdots\cdot$ x (t-k+1), x (t-k-1), $\cdots\cdot$ x (t-μ)) for some function

g of μ variables. (2) For each x (t-j); $k+1 \leq j \leq \mu$; that is non-idle in g there exists a distinct pair of unordered non-idle variables x $(t-p_j)$ and x $(t-q_j)$ such that $0 < p_j \leq k-1$ and $0 \leq q_j = p_j + k-j$ and such that every minterm in the canonical sum of products expansion of g contains x $(t-p_j) \cdot \overline{x\ (t-q_j)}$ or every minterm contains $\overline{x\ (t-p_j)} \cdot x\ (t-q_j)$.

Proof: As in the case of Theorem 5.5 the proof, although straightforward, is quite tedious. Therefore, proof will be omitted.

As in the case of the conditions sufficient for invertibility considered in Theorem 5.5 we cannot claim that Theorem 5.6 specifies output functions corresponding to all IL, binary, non-degenerate, FIM (μ) machines. There are such IL machines whose output functions do not conform to the requirements of Theorem 5.6. An example is the FSM whose output function is

$$y\ (t) = x\ (t-2) \oplus \overline{(x\ (t)} \cdot x\ (t-1) \cdot x\ (t-3) + x\ (t))\ .$$

This function may be associated with an IL (but not invertible), FIM (3) finite state machine.

We conclude this chapter by noting that, although Theorems 5.5 and 5.6 do not define output functions corresponding to all binary non-degenerate, FIM (μ), invertible and information lossless machines, these sufficient conditions do provide some indication as to the requisites of such output functions. We also remark that the requirement of both Theorems 5.5 and 5.6 that there exist some k such that the output function can be written

$$y\ (t) = x\ (t-k) \oplus g\ (x\ (t),\ x\ (t-1),\ \cdots\cdot x\ (t-k+1),\ x\ (t-k-1),\ \cdots\cdot x\ (t-\mu))$$

is believed to be a necessary condition for information losslessness. The proof for this conjecture has eluded us thus far, however.

CHAPTER VI

FINITE OUTPUT MEMORY MACHINES

A class of finite state machines for which properties of invertibility and information losslessness may be completely specified is that of finite output memory machines.

Definition 6.1: A finite state machine M has finite output memory μ (FOM(μ)) if μ is the least integer such that the output at time t can be expressed in the form

$$y(t) = f(x(t),\ y(t-1),\ y(t-2),\ \cdots\cdots\ y(t-\mu))$$

for $t \geq \mu$. If no such μ exists, then M is said to have infinite output memory.

The output function f is considered as a mapping;

$$f : X \times \bigcup_{i=1}^{N} Y^{\mu}(s_i) \longrightarrow Y ;$$

where N = #S. If an FSM has finite output memory μ, then any output sequence of length μ determines the final state up to equivalence.

Vairavan[1] has shown a necessary condition for any non-degenerate finite state machine to have finite output memory. This condition is given as

Lemma 6.1: If a non-degenerate FSM has finite output memory, then for all $s_i \in S$ and for all $x \neq u$, if $\lambda(s_i, x) = \lambda(s_i, u)$, then $\delta(s_i, x) = \delta(s_i, u)$.

[1]K. Vairavan, "On the Memory of Finite State Machines," Technical Report No. EE-683, University of Notre Dame, Dept. of Electrical Engineering, April 7, 1968, pp. 43-44.

We note that the condition of Lemma 6.1 is necessary for finite output memory whether or not the machine is minimal.

As a consequence of Lemma 6.1 we may state the following.

Theorem 6.1: A non-degenerate FSM M with finite output memory is IL if and only if $x \neq u$ implies that $\lambda(s_i, x) \neq \lambda(s_i, u)$ for every $s_i \in S$.

Proof: Sufficiency is obvious. Hence, we need only show necessity. Suppose M is IL but has a state s_i such that for $x \neq u$ we have $\lambda(s_i, x) = \lambda(s_i, u)$. If M is a non-degenerate FOM machine, it follows from Lemma 6.1 that $\delta(s_i, x) = \delta(s_i, u)$. But then M is not IL, contrary to our hypothesis and the theorem follows.

Since every machine with $\lambda(s_i, x) \neq \lambda(s_i, u)$ for every s_i is invertible with delay zero (INV #0) we may immediately state several corollaries.

Corollary 6.1.1: Every non-degenerate, FOM FSM is INV #0 and has an instantaneous inverse or is not invertible and has no inverse at all.

Corollary 6.1.2: In the case of non-degenerate, FOM FSM's information losslessness implies invertibility.

Furthermore, the result of Theorem 6.1 implies the following.

Corollary 6.1.3: For every IL, non-degenerate, FOM FSM with #X = #Y = q,

$$\# \bigcup_{s_i \in S} Y^n(s_i) = q^n$$

for every n.

Hence, from Corollary 6.1.3 it follows that if #X = #Y, then for every output sequence there exists a state that allows that output sequence on an IL, non-degenerate FOM machine.

As in the case of FIM (μ) machines an appropriate choice for the state set S of non-degenerate, FOM (μ) machines is the set of all possible output sequences of length μ. It follows that for IL machines of this class, the order of the state set S is q^{μ} if #X = #Y = q. Hence, for such machines, information losslessness implies strong connectedness.

We present one more result in this brief chapter. This result concerns the form of the output function associated with IL, non-degenerate, binary, FOM (μ) machines.

Theorem 6.2: A binary, non-degenerate, FOM (μ) FSM M is IL if and only if the output function f for M may be written in the form

$$y(t) = x(t) \oplus g(y(t-1), y(t-2), \cdots\cdots y(t-\mu)).$$

Proof: Sufficiency of the stated condition is evident by inspection. Hence, we need only show necessity. Suppose that no such function g exists. Then M must have a state, say s_i, such that $\lambda(s_i, 1) = \lambda(s_i, 0) = \alpha_0$. Let $s_i = (\alpha_1, \alpha_2, \cdots\cdots \alpha_{\mu})$ where the α_i are the μ past output digits. But the successor states of s_i satisfy $\delta(s_i, 0) = \delta(s_i, 1) = (\alpha_0, \alpha_1, \cdots\cdots \alpha_{\mu-1})$. Since two distinct input digits yield the same output and the same final state it is clear that M is not IL. Hence the existence of g such that

$$y(t) = x(t) \oplus g(y(t-1), y(t-2), \cdots\cdots y(t-\mu))$$

is a necessary condition for M to be IL and the theorem is proved.

CHAPTER VII

LINEAR MACHINES[1]

We consider in this chapter the most structured of all finite state machine classes, that of linear machines. In order to conform to somewhat more common usage we will refer to these devices as linear sequential circuits rather than linear finite state machines.

Definition 7.1: A finite state machine $M = \langle S, X, Y, \delta, \lambda \rangle$ is a linear sequential circuit (LSC) if S, X and Y are vector spaces over a finite field GF (q) and δ and λ satisfy

$$\underline{s}\,(t+1) = \delta(\underline{s}\,(t), \underline{x}\,(t)) = A\,\underline{s}\,(t) + B\,\underline{x}\,(t)$$

and

$$\underline{y}\,(t) = \lambda(\underline{s}\,(t), \underline{x}\,(t)) = C\,\underline{s}\,(t) + E\,\underline{x}\,(t)$$

where A, B, C, E are matrices over GF (q) and '+' is the additive operation in GF (q).

Since multiple input, multiple output LSC's will be considered we will let the input $\underline{x}\,(t)$ be a K dimensional column vector and the output $\underline{y}\,(t)$ be an N dimensional column vector; K = 1, 2, 3, ·····; N = 1, 2, 3, ····· . In addition, let the dimension of the state space be M; M = 1, 2, 3, ····· .

Since linear devices are considered in this chapter, it is possible to make use of transfer function matrices. It is well known that the transfer function

[1]The results of this chapter were previously presented in University of Notre Dame, Department of Electrical Engineering, Report No. 684, entitled, "Note on Feedforward Inverses for Linear Sequential Circuits", April 1, 1968.

matrix H (D), where D is the unit delay operator, completely describes the zero state response of an LSC. The zero state response is the only response we will consider here.

The matrix H (D) may be derived from the A, B, C and E structural matrices by a D-transformation of the equations given in Definition 7.1. The result of the derivation is

$$H(D) = E - C(DA - I_M)^{-1} DB \qquad (1)$$

where I_M is the M x M identity matrix. Clearly from Equation (1) the entries in H (D) are rational functions (ratios of polynomials in the delay operator D) with polynomial coefficients from GF (q). In addition, it may be seen from (1) that H (D) for an LSC with N outputs and K inputs is an N x K matrix.

As is well known an LSC is strongly connected if and only if it is state controllable[2]. Hence, the existence of an inverse with respect to state zero ($\underline{0}$) is equivalent to invertibility with respect to all states for state controllable LSC's. Moreover, a minimal realization of H (D) always results in a state controllable LSC. Hence, we lose no essential generality by restriction to state controllable response and we will use invertibility synonomously with inverse with respect to state $\underline{0}$ in the remainder of this chapter.

We will make use of the LSC transfer function matrix to derive the necessary and sufficient conditions for the existence of a special kind of inverse,

[2]Martin Cohn, "Controllability in Linear Sequential Networks", IRE Transactions on Circuit Theory, Vol. CT-9, No.1, March 1962, pp. 74-78.

i.e., a feedforward inverse LSC. Feedforward LSC's have transfer function matrices whose entries are all polynomials and can be realized by a feedback free connection of delay elements.

Motivated by the importance of feedforward inverse realizations for encoders of convolutional codes Massey and Sain[3] have derived a necessary and sufficient condition for the existence of such inverses in the case of feedforward LSC's. Their concern with feedforward LSC's arose from the fact that convolutional encoders are LSC's of this type. In this chapter we will extend their result to the entire class of linear sequential circuits. An interesting property of the extended inverse existence condition is that it specifies the minimum delay of any inverse circuit, feedforward or feedback, which may be realized. Furthermore, the existence condition given in this chapter incorporates an implicit procedure for the construction of feedforward inverses with minimal delay.

We begin our investigation of feedforward inverses for LSC's with the following conventions. Let H (D) represent the N x K transfer function matrix of some physically realizable LSC with N outputs and K inputs. Without loss of generality it may be assumed that the numerator and denominator polynomials of the entries in H (D) are relatively prime. Let the K dimensional column vector $\underline{I}$ (D) be defined as the vector whose k-th component is the

[3]J. L. Massey and M. K. Sain, "Inverses of Linear Sequential Circuits", IEEE Transactions On Electronic Computers, Vol. C-17, April 1968, pp. 330-337. (See also "Postscript to Inverses of Linear Sequential Circuits", IEEE Transactions on Computers, Vol. C-17, Dec. 1968, pp. 1177).

D-transform of the k-th input sequence; $k = 1, 2, \cdots\cdots K$; and let $\underline{T}(D)$ be an N-dimensional column vector whose n-th component is the transform of the n-th output sequence; $n = 1, 2, \cdots\cdots N$. Then if the LSC whose transfer function matrix is $H(D)$ is in the zero initial state we have

$$\underline{T}(D) = H(D)\,\underline{I}(D) \quad . \tag{2}$$

An LSC is invertible, possibly with delay, if and only if $\underline{I}(D)$ can be uniquely recovered from $\underline{T}(D)$. Clearly a necessary and sufficient condition for unique recovery is

$$\text{rank}\,(H(D)) = K \tag{3}$$

where the entries in $H(D)$ are considered as elements in the field of rational functions over GF (q). Condition (3) requires that

$$N \geq K \quad . \tag{4}$$

Since interest is confined to those LSC's which are invertible, condition (4) will be assumed in all that follows.

If condition (3) holds there exists a $K \times N$ matrix $R(D)$ of rational functions (not unique if $N > K$) such that

$$R(D)\,H(D) = I_K \tag{5}$$

where I_K is the $K \times K$ identity matrix. Note that an $R(D)$ which satisfies (5) may not be realizable since some entries or $R(D)$ may have denominator polynomials which contain D as a factor. Again we assume that the numerator and denominator of each entry in $R(D)$ are relatively prime. Let L be the greatest power of D which is a factor of a denominator polynomial. It is always possible

to obtain a transfer function matrix $R'(D)$ which is physically realizable by multiplying $R(D)$ by D^L.

$$R'(D) = D^L R(D) \tag{6}$$

With this definition of $R'(D)$ and L, multiplication of both sides of (5) by D^L gives

$$R'(D) H(D) = D^L I_K \tag{7}$$

which in turn from (2) implies

$$R'(D) \underline{T}(D) = D^L \underline{I}(D) \quad . \tag{8}$$

Hence, $R'(D)$ is the transfer function matrix of a realizable, delay L inverse for the LSC whose transfer function matrix is $H(D)$. A transfer function matrix has a feedforward realization if and only if all its entries are polynomials rather than more general rational functions. Thus, the search for feedforward inverses is essentially the search for $K \times N$ matrices $R'(D)$ which satisfy Equation (8) and whose entries are all polynomials.

Let $Q(D) = Q_0 + Q_1 D + \cdots\cdots + Q_m D^m$ be the least common multiple (lcm) of the denominator polymonials of the entries of $H(D)$. Since $H(D)$ is characteristic of a realizable circuit, it follows that $Q_0 \neq 0$. With $Q(D)$ so defined there exists an $N \times K$ matrix of polymonials $G(D)$ such that

$$H(D) = G(D) / Q(D) \quad . \tag{9}$$

The matrix $G(D)$ has $\binom{N}{K}$ distinct $K \times K$ submatrices. Let $G(D)_n$ denote the n-th $K \times K$ submatrix of $G(D)$ and let $\Delta_n(D)$ be the determinant of $G(D)_n$. In addition, let $C(D)_n$ be the adjoint matrix of $G(D)_n$ and let $c_{ij}(D)_n$; $i = 1, 2, \cdots\cdots K$; $j = 1, 2, \cdots\cdots K$; represent the polynomial entries in $C(D)_n$. Each

$C(D)_n$ has K^2 entries which are the K^2 cofactors of $G(D)_n$. Note that the entries $c_{ij}(D)_n$; $n = 1, 2, \cdots \binom{N}{K}$; are not all distinct but each appears N-K+1 times.

With these preliminaries completed, the main result of this chapter may be presented as the following theorem.

Theorem 7.1[4]: An N-output, K-input linear sequential circuit with transfer function H (D) has a feedforward inverse if and only if

$$\frac{\Delta(D)}{\gcd\left[\Delta(D),\ Q(D)\right]\ C(D)} = \frac{D^L}{\beta(D)} \tag{10}$$

where $\Delta(D) = \gcd\left[\Delta_i(D)\right]$; $i = 1, 2, \cdots \binom{N}{K}$;

$C(D) = \gcd\left[c_{ij}(D)_n\right]$; $i = 1, 2, \cdots K$; $j = 1, 2, \cdots K$; $n = 1, 2, \cdots \binom{N}{K}$;

L is an integer ≥ 0, $\beta(D)$ is a polynomial with $\beta(0) \neq 0$, and "gcd" indicates "greatest common divisor". Moreover, there exists a feedforward inverse with delay exactly L and no inverse of any kind exists with delay less than L.

Note that $L < 0$ can never occur since $Q(0) \neq 0$ and $C(D)$ divides $\Delta(D)$.

The proof of Theorem 7.1 will be given in three parts, showing successively the necessity, the sufficiency and the minimality of the delay L defined by condition (10).

[4]The result of this theorem was communicated to Dr. G. D. Forney who subsequently gave an elegant algebraic proof using the Smith-McMillan canonical matrix expansion of the transfer function matrix H (D). See: G. D. Forney, "Convolutional Codes I : Algebraic Structure", IEEE Transactions on Information Theory, Vol. IT-16, No. 6, Nov. 1970, to appear.

Proof of Necessity: Suppose (10) is not satisfied for any $L \geq 0$ and for any $\beta(D)$ with $\beta(0) \neq 0$. Then

$$\frac{\Delta(D)}{\gcd\left[\Delta(D),\ Q(D)\right] C(D)} = \frac{\alpha(D)}{\beta(D)} \tag{11}$$

where $\alpha(D)$ is a polynomial containing an irreducible factor, say m (D), such that deg $\left[m(D)\right] \geq 1$ and $m(0) \neq 0$. But then $\Delta(D)$ also has m (D) as a factor. Let the multiplicity of m (D) as a factor of $\Delta(D)$ be δ where $\delta \geq 1$. Since both gcd $\left[\Delta(D),\ Q(D)\right]$ and C (D) may have m (D) as a factor, let μ be the multiplicity of m (D) as a factor of gcd $\left[\Delta(D),\ Q(D)\right]$ and let λ be the multiplicity of m (D) as a factor of C (D). Note that since $\delta \geq 1$, it follows that μ is the multiplicity of m (D) as a factor of Q (D). Now both $\mu \geq 0$ and $\lambda \geq 0$ and by hypothesis $\alpha(D)$ has m (D) as a factor, therefore, the multiplicities satisfy

$$\delta > \mu + \lambda \ . \tag{12}$$

If C (D) has $m^{\lambda}(D)$ as a factor, there exists some K x K submatrix of G (D) whose adjoint has a row in which the elements have a greatest common divisor divisible by $m^{\lambda}(D)$ but not by $m^{\lambda+1}(D)$. Let the submatrix whose adjoint contains this row be $G(D)_n$ and let the adjoint matrix be $C(D)_n$. Let the r-th row of $C(D)_n$ contain an element which has m (D) as a factor of multiplicity precisely λ.

Define the polynomial $P_r(D)$ as the greatest common divisor of the K entries in the r-th row of $C(D)_n$. Then there exist polynomials $F_i(D)$; $i = 1, 2, \cdots\cdots K$; such that

$$P_r(D) = c_{r1}(D)_n F_1(D) + c_{r2}(D)_n F_2(D) + \cdots\cdots + c_{rK}(D)_n F_K(D) \tag{13}$$

where the $c_{ri}(D)_n$ are the entries in the r-th row of $C(D)_n$. Define the polynomial vector, $\underline{P}(D) = (P_1(D), P_2(D) \cdots\cdots, P_K(D))$, from the following.

$$\underline{P}(D) = C(D)_n \underline{F}(D) \tag{14}$$

In (14) the polynomial vector, $\underline{F}(D) = (F_1(D), F_2(D), \cdots\cdots, F_K(D))$, is defined by (13). Premultiplication of both sides of (14) by $G(D)_n$ gives

$$G(D)_n \underline{P}(D) = \Delta_n(D) \underline{F}(D) \tag{15}$$

since

$$G(D)_n C(D)_n = C(D)_n G(D)_n = \Delta_n(D) I_K \tag{16}$$

where I_K is the K x K identity matrix.

Now suppose that the K inputs to an LSC whose transfer function matrix is G (D) are given by

$$I_i(D) = \frac{P_i(D) Q(D)}{m^{\mu+\lambda+1}(D)}; \quad i = 1, 2, \cdots\cdots K \ . \tag{17}$$

Note that at least one input sequence defined by (17), namely the sequence corresponding to $I_r(D)$, has an infinite number of non-zero digits since $P_r(D)$ and $Q(D)$ have $m(D)$ as a factor with respective multiplicities of exactly λ and μ. Solving (17) for $P_i(D)$, the result is

$$P_i(D) = I_i(D)\, m^{\mu+\lambda+1}(D)/Q(D) \ . \tag{18}$$

The following lemma due to Massey and Sain[3] is useful in demonstration of the necessity of Condition (10).

Lemma 7.1: For any polynomial vector $\underline{P}(D)$ satisfying (15) and for any index j; $1 \leq j \leq N$; the j-th row of G (D) satisfies

$$\sum_{i=1}^{K} G_{ji}(D) P_i(D) = \Delta(D) A_j(D) \tag{19}$$

where the $G_{ji}(D)$ are the entries in the j-th row of $G(D)$ and $A_j(D)$ is a polynomial.

Substitution of (18) in (19) gives

$$\frac{1}{Q(D)} \sum_{i=1}^{K} G_{ji}(D)\, I_i(D) = \frac{\Delta(D)\, A_j(D)}{m^{\mu+\lambda+1}(D)} . \tag{20}$$

But the left hand side of (20) is

$$\sum_{i=1}^{K} H_{ji}(D)\, I_i(D) = T_j(D) \tag{21}$$

where the $H_{ji}(D)$; $i = 1, 2, \cdots, K$; are the entries in the j-th row of $H(D)$. Thus

$$T_j(D) = \frac{\Delta(D)\, A_j(D)}{m^{\mu+\lambda+1}(D)} . \tag{22}$$

Recall that $\Delta(D)$ contains a factor $m(D)$ with multiplicity δ and (12) states that $\delta > \mu+\lambda$. Therefore, $m^{\mu+\lambda+1}(D)$ divides $\Delta(D)$. It follows that $T_j(D)$ has only a finite number of non-zero digits for every j. Thus, by the following result of Massey and Sain[3], the LSC whose outputs are defined by (22) when the inputs are given by (17) has no feedforward inverse.

Lemma 7.2: If for a given LSC there exists an input sequence with infinitely many non-zero digits such that the corresponding output sequence has only finitely many non-zero digits, then the LSC has no feedforward inverse, with delay or without delay.

Consequently, when (10) is not satisfied (or $\alpha(D) \neq D^L$) no feedforward inverse circuit exists.

Proof of Sufficiency: Suppose that for a given LSC with transfer function matrix H (D) Condition (10) is satisfied for some $L \geq 0$. Since $\Delta(D) = \gcd\left[\Delta_1(D), \Delta_2(D), \cdots \Delta_{\binom{N}{K}}(D)\right]$, there exist polynomials $B_i(D)$ such that

$$\sum_{i=1}^{\binom{N}{K}} B_i(D)\, \Delta_i(D) = \Delta(D) \quad . \tag{23}$$

Therefore, by use of (16)

$$\sum_{i=1}^{\binom{N}{K}} B_i(D)\, C(D)_i\, G(D)_i = \Delta(D)\, I_K \quad . \tag{24}$$

But if Condition (10) is satisfied (24) gives

$$\sum_{i=1}^{\binom{N}{K}} B_i(D)\, C(D)_i\, G(D)_i = \frac{\gcd\left[\Delta(D), Q(D)\right] C(D)\, D^L}{\beta(D)} I_K \quad . \tag{25}$$

In addition, if $\underline{T}(D)_i$ is a vector of K output sequences corresponding to the rows used to form $G(D)_i$, it is clear that

$$G(D)_i \underline{I}(D) = Q(D)\, \underline{T}(D)_i \quad . \tag{26}$$

By use of (26) Equation (25) becomes

$$\beta(D)\, Q(D) \sum_{i=1}^{\binom{N}{K}} B_i(D)\, C(D)_i\, \underline{T}(D)_i = \gcd\left[\Delta(D), Q(D)\right] C(D)\, D^L \underline{I}(D) \quad . \tag{27}$$

But gcd $\left[\Delta(D), Q(D)\right]$ divides $Q(D)$ and $C(D)$ divides each entry of $C(D)_i$. Hence, we may define the polynomial

$$Q'(D) = Q(D)/\text{gcd}\left[\Delta(D), Q(D)\right] \tag{28}$$

and define the matrix of polynomials

$$C'(D)_i = C(D)_i/C(D) \quad . \tag{29}$$

Then Equation (27) becomes

$$\beta(D)\, Q'(D) \sum_{i=1}^{N_K} B_i(D)\, C'(D)_i\, \underline{T}(D)_i = D^L \underline{I}(D) \quad . \tag{30}$$

Now Equation (30) gives an implicit formulation for the transfer function of an inverse LSC with delay, L. Note that each $\underline{T}(D)_i$ in the summation on the left hand side of (30) is multiplied by a K x K matrix of polynomials. Clearly, the summation of polynomials which multiply each transformed sequence $T_j(D)$ results in a polynomial. It follows that the inverse constructed from (30) is a feedforward inverse. Thus, Condition (10) has been shown to be sufficient for the existence of a feedforward inverse LSC with delay L.

It should be noted that (30) does not give a unique feedforward realization since the set of $B_i(D)$ which satisfy (23) are not unique.

Proof of Minimal Delay: Condition (10) has been shown to be necessary and sufficient for the existence of a feedforward inverse LSC of delay L. To complete the proof of the theorem, it remains to show that no inverse with delay less than L exists. To aid in establishing this result the following

lemma where $\underline{i}$ (t) is the vector of K inputs at time t and $\underline{t}$ (t) is the vector of N outputs, is useful.

Lemma 7.3: If for a given LSC there exists an input vector sequence with $\underline{i}$ (0) $\neq \underline{0}$ such that the corresponding output vector sequence has $\underline{t}$ (0) = $\underline{t}$ (1) = ····· $\underline{t}$ (L-1) = $\underline{0}$, then no inverse (of any kind) with delay less than L exists.

Proof: Suppose the all zero vector sequence is applied to an LSC in its zero state such that $\underline{i}$ (t) = $\underline{0}$ for all t. The corresponding output vector sequence is also the all zero vector sequence and in particular, $\underline{t}$ (0) = $\underline{t}$ (1) = ····· $\underline{t}$ (L-1) = $\underline{0}$. But if some other input vector sequence with $\underline{i}$ (0) $\neq \underline{0}$ also results in an output vector sequence such that $\underline{t}$ (t) = $\underline{0}$ for $0 \leq t \leq L-1$, then the output vector sequences are identical in the first L time units for two distinct input vector sequences. Clearly no inverse can differentiate between the two output vector sequences until t = L. Therefore, no inverse with delay less than L exists. Hence, the lemma is proved.

It now suffices to show that, if Condition (10) is satisfied, there exists an input vector sequence for which $\underline{i}$ (0) $\neq \underline{0}$ and a corresponding output vector sequence such that $\underline{t}$ (0) = $\underline{t}$ (1) = ····· = $\underline{t}$ (L-1) = $\underline{0}$. To this end suppose Condition (10) is satisfied. Then $\Delta(D)/(\text{gcd } [\Delta(D), Q(D)]$ C (D)) has D^L as a factor. Since Q (0) $\neq$ 0, D does not divide gcd $[\Delta(D), Q(D)]$, but may divide C (D). Therefore, let C (D) have D as a factor with multiplicity $k \geq 0$. Proceeding as in the proof of necessity, there exists some $C(D)_i$ which contains a row, say the r-th, in which the entries have a greatest common divisor which is divisible by D^k. Let this greatest common divisor be $P_r(D)$.

Define the polynomial vector, $\underline{P}(D)$, as in Equation (14) and consider the function, $P_i(D)\, Q(D)/(\gcd\left[\Delta(D),\, Q(D)\right] C(D))$. Observe that neither $Q(D)$ nor $\gcd\left[\Delta(D),\, Q(D)\right]$ contains D as a factor. In addition, there exists some $P_i(D)$, namely $P_r(D)$, which has D^k as a factor. Since $C(D)$ has D as a factor of multiplicity k, it follows that $P_r(D)\, Q(D)/(\gcd\left[\Delta(D),\, Q(D)\right] C(D))$ does not contain D as a factor. Thus, if $I_i(D)$ is defined by

$$I_i(D) = \frac{P_i(D)\, Q(D)}{\gcd\left[\Delta(D),\, Q(D)\right] C(D)}\,; \quad i = 1,\ 2,\ \cdots\cdots\ K; \tag{31}$$

it is seen that $\underline{i}(0) \neq \underline{0}$ for the transformed input sequences defined by (31). Now solution of (31) for $P_i(D)$ and substitution in (19) gives

$$T_j(D) = \sum_{i=1}^{K} \frac{G_{ji}(D)\, I_i(D)}{Q(D)} = \frac{\Delta(D)\, A_j(D)}{\gcd\left[\Delta(D),\, Q(D)\right] C(D)}\,. \tag{32}$$

But, by hypothesis, Condition (10) is satisfied for some $L \geq 0$. Therefore

$$T_j(D) = \frac{D^L A_j(D)}{\beta(D)} \tag{33}$$

for all j. Since $\beta(0) \neq 0$ and $A_j(D)$ is a polynomial for each j, it is clear that the output sequences corresponding to (33) have $\underline{t}(0) = \underline{t}(1) = \underline{t}(2) = \cdots\cdots = \underline{t}(L-1) = \underline{0}$. Hence, by Lemma 7.3 it is concluded that no inverse with delay less than L exists. Note that the delay which is defined by (10) is minimal over all classes of linear inverse circuits, not just feedforward inverses. It follows that no inverse of any kind with delay less than L exists. This completes the proof of the theorem.

The results embodied in Theorem 7.1 are threefold. First, the theorem gives a necessary and sufficient condition for any LSC to have a feedforward

inverse. Secondly, an implicit procedure for the construction of feedforward inverses, when they exist, results from the proof of the theorem. A non-trivial application of the construction procedure is given in Appendix A. Finally, the condition of the theorem defines the minimum delay L of any inverse, i.e., no inverse of any kind with smaller delay exists.

CHAPTER VIII

UPPER BOUNDS ON INVERSE DELAY

In this chapter we consider upper bounds on inverse delay or on the integer L for INV #L finite state machines. Bounds will be considered in terms of the order of the state set for the general class of FSM's as well as for the special case of binary machines. An upper bound on inverse delay for any invertible machine with N states is well known and can be obtained quite simply. It can be shown that every INV #L machine satisfies $L \leq N(N-1)/2$ as a direct consequence of Even's[1] test for IL and ILF behavior (see Chapter III). The least order of losslessness of an ILF machine M is given by the number of nodes on the longest chain of distinct compatible pairs (nodes) of distinct states on the invertibility test graph (ITG) for M. By Theorem 3.1 M is INV #L if and only if L is the least integer such that M is ILF of order L. Clearly an upper bound on L for an N state, INV #L machine is given by the maximum possible number of distinct compatible pairs of distinct states on the ITG. Hence, for any N state, INV #L machine, $L \leq \binom{N}{2} = N(N-1)/2$. We will show shortly that in the general case this is a tight upper bound, i.e., for every N these exist N state, INV #L machines with $L = N(N-1)/2$.

It is possible, however, to improve on this bound in certain restricted cases. To accomplish this, we will make use of the following definition.

[1]S. Even, "On Information Lossless Automata of Finite Order", IEEE Transactions on Electronic Computers, Vol. EC-14, August 1965, pp. 561-569.

Definition 8.1: A state s_i is an n-lossless state if n is the least integer such that there exist no x^n and u^n with different first letters such that $\lambda(s_i, x^n) = \lambda(s_i, u^n)$.

We observe that every state on an INV #L FSM is n-lossless for some $n \leq L+1$ and that there must exist at least one state that is (L+1)-lossless. If every state is n-lossless for some n, then L = n-1.

Making use of Definition 8.1 we may state

Lemma 8.1: If a strongly connected FSM M is INV #L for $L \geq 1$ and if #X = #Y = q, then there exists no length L sequence of one-lossless states.

Proof: The lemma follows directly from Theorem 2.1 since the existence of a sequence of one-lossless states of length L or longer implies that for some $\alpha^L \in Y^L$, $\#S_f(s_0, \alpha^L) = 1$ where s_0 is the first one-lossless state in the sequence. By Theorem 2.1 it follows that $\#S_f(s, y^L) = 1$ for every $s \in S$ and $y^L \in Y^L(s)$. Hence, either every state is one-lossless and L = 0 or M is not INV #L.

In the case for which q is prime we may rephrase Lemma 8.1 to further restrict the length of any sequence of one-lossless states. For machines which satisfy the hypothesis of Lemma 8.1 with the added restriction that q is prime we have by the corollary of Theorem 2.2 that $\#S_f(s, y^L) = q^j$ for some $j \geq 1$ and for every s and y^L. It follows that there can exist no sequence of one-lossless states of length longer than L-j on such machines. Hence, we

conclude that if a strongly connected FSM M is INV #L for $L \geq 1$ and if #X = #Y = q for q a prime integer and if $\#S_f(s_0, \alpha^L) = q^j$ for some s_0 and α^L, then there can exist no sequence of one-lossless states of length longer than L-j.

We turn now to the primary consideration of this chapter, i.e., upper bounds on inverse delay. For the restricted, but important, class of binary machines which satisfy

$$\underset{s,\, y^L}{\text{MAX}} \#S_f(s,\, y^L) = 2$$

it is possible to derive a tight upper bound on inverse delay which increases only linearly with the order of the state set. To aid in the derivation we make use of the following two results.

Lemma 8.2: If an FSM M is IL and if #X = #Y = q, then for every $n \geq 0$

$$\underset{s,\, y^n}{\text{MAX}} \#S_f(s,\, y^n) \leq \underset{s,\, y^{n+1}}{\text{MAX}} \#S_f(s,\, y^{n+1}) \quad .$$

Proof: Let s_i and α^n satisfy

$$\#X^n(s_i,\, \alpha^n) = \underset{s,\, y^n}{\text{MAX}} \#X^n(s,\, y^n) = K_n \quad .$$

Since #X = q we may state

$$\sum_y \#X^{n+1}(s_i,\, \alpha^n\, y) = q\, K_n \quad .$$

However, since #Y = q it follows that

$$\underset{y}{\text{MAX}} \#X^{n+1}(s_i,\, \alpha^n\, y) \geq K_n \quad .$$

But it is always true that

$$\underset{y}{\text{MAX}}\ \#X^{n+1}(s_i, \alpha^n y) \leq \underset{s,\, y^{n+1}}{\text{MAX}}\ \#X^{n+1}(s, y^{n+1}) \ .$$

Hence, it follows that

$$\underset{s,\, y^n}{\text{MAX}}\ \#X^{n}(s, y^{n}) \leq \underset{s,\, y^{n+1}}{\text{MAX}}\ \#X^{n+1}(s, y^{n+1})$$

and from the IL property we may conclude

$$\underset{s,\, y^n}{\text{MAX}}\ \#S_f(s, y^{n}) \leq \underset{s,\, y^{n+1}}{\text{MAX}}\ \#S_f(s, y^{n+1}) \ .$$

Therefore, the lemma is proved.

Another useful preliminary result is given as

Lemma 8.3: If M is a binary, INV #L FSM which satisfies

$$\underset{s,\, y^L}{\text{MAX}}\ \#S_f(s, y^{L}) = 2,$$

then no state which initiates a length L sequence of one-lossless states can be included in any compatible pair on the ITG for M.

Proof: Suppose state s_i is the first state in a length L sequence of one-lossless states. Suppose further that s_i is included in some compatible pair on the ITG for M. Let (s_i, s_k) be this compatible pair. Let n be the least integer such that there exists s_0 and α^n such that both s_i and $s_k \in S_f(s_0, \alpha^n)$. Since $L \geq n$, it follows from the hypothesis of the theorem and from Lemma 8.2 that $\#S_f(s_0, \alpha^n) = 2$. Since s_i is one-lossless, there must exist β such that both s_i and $s_k \in S_i(\beta)$. Hence, $L \geq n+1$ and $\#S_f(s_0, \alpha^n \beta) = 2$. Consequently, s_k is a one-lossless state also. Since s_i is the first state in a length L sequence

of one-lossless states, there exists a successor of s_i that is one-lossless and on the assumed length L sequence of one-lossless states. Let this successor be $\delta(s_i, a)$. But $S_f(s_0, \alpha^n y) = 2$ for every y. Hence, there exists a successor of s_k, say $\delta(s_k, b)$, such that both $\delta(s_i, a)$ and $\delta(s_i, b) \in S_f(s_0, \alpha^n \gamma)$ where $\gamma = \beta$ or $\bar{\beta}$ since M is binary. However, because $\delta(s_i, a)$ is one-lossless it follows that $L \geq n+2$ and consequently that $\#S_f(s_0, \alpha^n \gamma y) = 2$ for every y and that there exists a successor of $\delta(s_i, a)$ that is one-lossless. Clearly a continuation of the indicated arguments yields the conclusion that $L \geq n+m$ for arbitrarily large m. Therefore, no state which initiates a length L sequence of one-lossless states can be included in a compatible pair on the ITG for M and the lemma is proved.

Based on the preceding two preliminary results it is possible to show an upper bound on inverse delay for the class of machines considered.

Theorem 8.1: If M is an N state, binary, INV #L FSM which satisfies

$$\underset{s, y^L}{\text{MAX}} \#S_f(s, y^L) = 2,$$

then $L \leq N/2$.

Proof: The fact that M is INV #L implies that there exists $s_0 \in S$ and $a^L = a_1 a_2 \cdots a_L$ and $b^L = b_1 b_2 \cdots b_L$ with $a_1 \neq b_1$ such that $\lambda(s_0, a^L) = \lambda(s_0, b^L)$. Suppose $L > N/2$. This requires that at least one of the following conditions is satisfied for $i < j \leq L$.

(1) $\delta(s_0, a_1 a_2 \cdots a_i) = \delta(s_0, a_1 a_2 \cdots a_j)$

(2) $\delta(s_0, b_1 b_2 \cdots b_i) = \delta(s_0, b_1 b_2 \cdots b_j)$

(3) $\delta(s_0, a_1 a_2 \cdots a_i) = \delta(s_0, b_1 b_2 \cdots b_j)$

(4) $\delta(s_0, b_1 b_2 \cdots b_i) = \delta(s_0, a_1 a_2 \cdots a_j)$

The first two conditions differ only in an arbitrary assignment of input labels. Consequently, we need not consider condition (2). A similar conclusion is reached by comparison of conditions (3) and (4). Hence, we need not consider condition (4).

Suppose condition (1) holds. Since M is binary and since

$$\underset{s, y^L}{\text{MAX}} \#S_f(s, y^L) = 2,$$

it follows from Lemma 8.2 that all states $\delta(s_0, a_1 a_2 \cdots a_k)$ and $\delta(s_0, b_1 b_2 \cdots b_k)$ are one-lossless for every k; $1 \leq k < L$. In addition, since $\delta(s_0, a_1 a_2 \cdots a_i) = \delta(s_0, a_1 a_2 \cdots a_j)$, there exists an infinite length sequence of one-lossless states starting from state $\delta(s_0, a_1)$. But $\delta(s_0, a_1)$ and $\delta(s_0, b_1)$ form a compatible pair on the ITG for M. Hence, by Lemma 8.3, M is not INV #L for any L.

Suppose condition (3) holds. This case is illustrated in Figure 8.1.

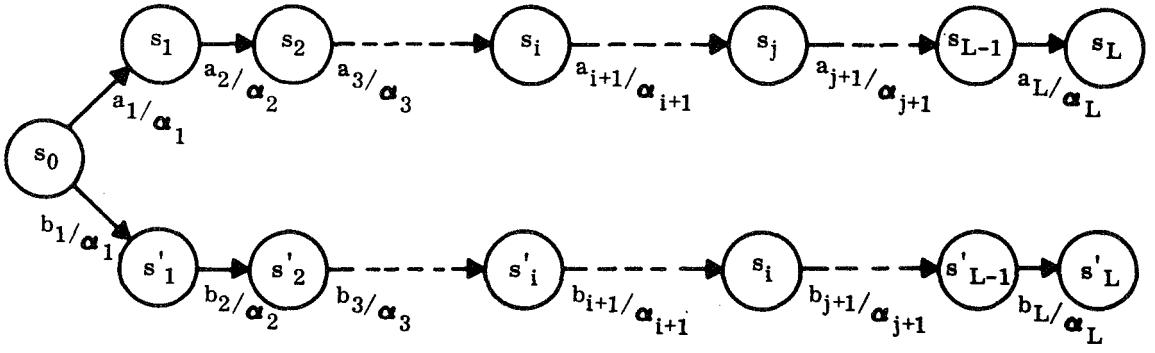


FIGURE 8.1 - TWO LENGTH L STATE SEQUENCES WITH COMMON OUTPUT LABELS AND A COMMON INCLUDED STATE

We note that it is not possible that i = j since this implies that M is not IL. By the same arguments as were employed in the case of condition (1) it follows

that $\delta(s_0, a_1 a_2 \cdots a_k)$ and $\delta(s_0, b_1 b_2 \cdots b_k)$ are one-lossless states for every k; $1 \leq k < L$. But then, since $\delta(s_0, a_1 a_2 \cdots a_i) = \delta(s_0, b_1 b_2 \cdots b_j)$, we have that $\delta(\delta(s_0, b_1 b_2 \cdots b_j), a_{i+1} a_{i+2} \cdots a_k)$ is a one-lossless state for every k; $i+1 \leq k < L$. But this implies that there exists a sequence of one-lossless states of length L+j-i starting from state $\delta(s_0, b_1)$. Since $j > i$ the length of the sequence is greater than L. By construction $(\delta(s_0, a_1), \delta(s_0, b_1))$ is a compatible pair on the ITG for M. Hence, by Lemma 8.3, M is not INV #L. Consequently, neither conditions (1) nor (3) are compatible with the hypothesis of the theorem and it follows that $L \leq N/2$.

The bound on inverse delay for machines satisfying the conditions of Theorem 8.1 is tight since we can show examples of such machines which satisfy L = N/2 for any L. The N state machine defined by the state transition table of Figure 8.2 meets the bound with equality.

S \ X	0	1
s_1	s_3 1	s_4 1
s_2	s_3 0	s_4 0
s_3	s_5 1	s_6 0
s_4	s_5 0	s_6 1
⋮		
s_i	s_{i+2} 1	s_{i+3} 0
s_{i+1}	s_{i+2} 0	s_{i+3} 1
⋮		
s_{N-1}	s_1 1	s_2 0
s_N	s_1 0	s_2 1

FIGURE 8.2 - A BINARY, INV #L, N STATE FINITE STATE MACHINE WITH L = N/2 AND MAX $\#S_f(s, y^L) = 2$
s, y^L

We observe that machines defined as in Figure 8.2 are strongly connected. Hence, it is possible to find a strongly connected, binary, INV #L machine with 2L states for every integer L. We remark further that it is possible to show the existence of such machines with 2L states with $\underset{s,\, y^L}{\text{MAX}} \#S_f(s,\ y^L) = 2^j$ for j = 2 as well as for j = 1. The series of binary, strongly connected invertible machines defined as in Figure 8.3 satisfy $\#S_f(s,\ y^L) = 4$ and L = N/2 for every L = 2, 3, 4, ····· . We have been unable to find such examples satisfying $\#S_f(s,\ y^L) = 2^j$ and L = N/2 for $j \geq 3$, however,

In general, the bound on inverse delay for binary, strongly connected, invertible machines appears to depend on $\#S_f(s,\ y^L)$. It is conjectured that the tightest possible bound on inverse delay for such machines is given by

$$L \leq N/2 - 2^{j-1} + j$$

where N = #S and $\#S_f(s,\ y^L) = 2^j$.

We have no proof of this suspected upper bound as yet. It can be seen that for j = 1, 2 the conjectured bound reduces to $L \leq N/2$ which is consistent with our previous results and examples. For j = 3, 4 several examples have been found for which L meets the conjectured bound with equality. No binary, strongly connected machines have been found such that L exceeds the bound, however.

For more general classes of invertible finite state machines we assert that it is possible to meet the bound on inverse delay $L = \binom{N}{2}$ with equality if arbitrary orders of input and output alphabets are allowed. For any N,

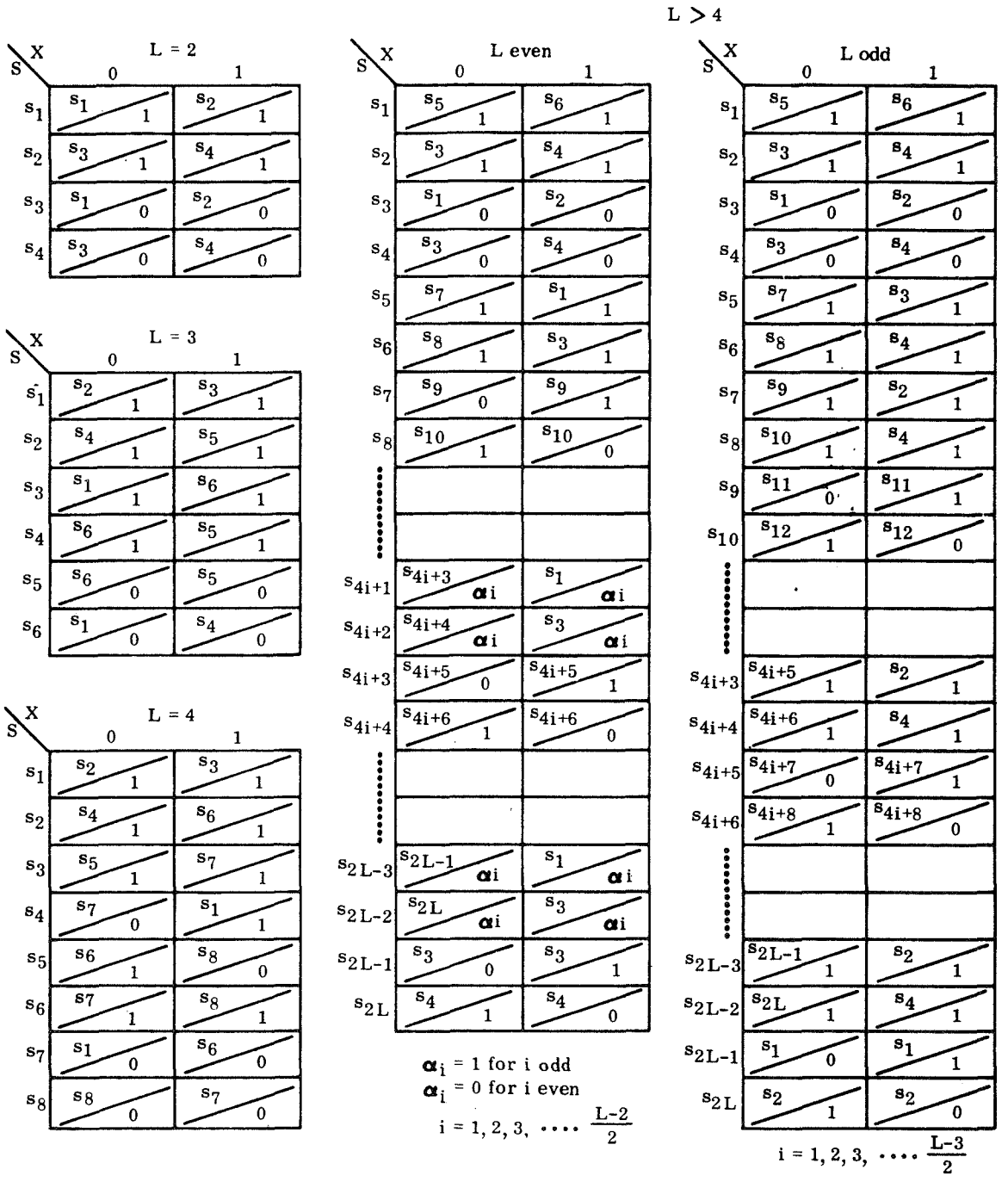


FIGURE 8.3 - BINARY, INV #L, STRONGLY CONNECTED FINITE STATE MACHINES SATISFYING $\#S_f(s, y^L) = 4$ AND L = N/2 FOR L = 2, 3, 4, ...

examples may be constructed which show the validity of this assertion. Moreover, it is possible to demonstrate a general form for finite state machines which satisfy $L = \binom{N}{2}$ for any N. One such trivial, but valid, construction is given in Figure 8.4. The 2N undefined transitions on the right hand side of the state transition diagram of Figure 8.4 may be labelled with any of the N states. The 2N output labels corresponding to unlabelled transitions should all be distinct and not appear anywhere else on the diagram. Since the machine of Figure 8.4 is INV $\#\binom{N}{2}$ and has N states we have shown by construction that

Theorem 8.2: For every N there exists an INV #L finite state machine with N states such that $L = \binom{N}{2}$.

Finite state machines formulated in the manner of Figure 8.4 satisfy $\#X = N+1$ and $\#Y = \binom{N}{2} + 2N$. It is expected that more economical (in terms of input and output set orders) realizations of machines which satisfy $L = \binom{N}{2}$ may be found. It is possible, for instance, to construct an INV #3 binary input, ternary output machine with three states. The state transition diagram for such a machine is shown in Figure 8.5.

We present in this chapter one more result; a result which gives a necessary condition for any FSM to be INV #L for $L > N$. We state this condition as

Theorem 8.3: If M is an INV #L finite state machine with $L > N$, then there can exist no $s_0 \in S$ and $a^L = a_1\, a_2 \cdots a_L$ and $b^L = b_1\, b_2 \cdots b_L$ with $a_1 \neq b_1$ such that $\lambda(s_0, a^L) = \lambda(s_0, b^L) = \alpha_1\, \alpha_2 \cdots \alpha_L$ and such that $\alpha_i = \alpha_j$ for every i, j satisfying $i < j \leq L$.

S \ X	1	2	3	4	5	.....	N-3	N-2	N-1	N	N+1
s_1	s_2 / 1	s_1 / 1	s_1 / 2	s_1 / 3	s_1 / 4		s_1 / N-4	s_1 / N-3	s_1 / N-2	s_1 / N-1	s_2 / N
s_2	s_3 / 2	s_2 / N+1	s_2 / N+2	s_2 / N+3	s_2 / N+4		s_2 / 2N-4	s_2 / 2N-3	s_3 / 2N-2		
s_3	s_4 / 3	s_4 / N+1	s_3 / 2N-1	s_3 / 2N	s_3 / 2N+1		s_3 / 3N-7	s_3 / 3N-6	s_4 / 3N-5		
s_4	s_5 / 4	s_5 / N+2	s_5 / 2N-1	s_4 / 3N-4	s_4 / 3N-3		s_4 / 4N-11	s_4 / 4N-12	s_5 / 4N-9		
s_5	s_6 / 5	s_6 / N+3	s_6 / 2N	s_6 / 3N-4	s_5 / 4N-8		s_5 / 5N-16	s_5 / 5N-15	s_6 / 5N-14		
s_6	s_7 / 6	s_7 / N+4	s_7 / 2N+1	s_7 / 3N-3	s_7 / 4N-8		s_6 / 6N-22	s_6 / 6N-21	s_7 / 6N-20		
.....											
s_i	s_{i+1} / i	s_{i+1} / N+i-2	s_{i+1} / 2N+i-5	s_{i+1} / 3N+i-9	s_{i+1} / 4N+i-14		s_i / $iN-2-\sum_{j=2}^{i} j$	s_i / $iN-1-\sum_{j=2}^{i} j$	s_{i+1} / $iN-\sum_{j=2}^{i} j$		
.....											
s_{N-2}	s_{N-1} / N-2	s_{N-1} / 2N-4	s_{N-1} / 3N-7	s_{N-1} / 4N-11	s_{N-1} / 5N-16		s_{N-1} / $\binom{N}{2}-4$	s_{N-2} / $\binom{N}{2}-1$	s_{N-1} / $\binom{N}{2}$		
s_{N-1}	s_N / N-1	s_N / 2N-3	s_N / 3N-6	s_N / 4N-10	s_N / 5N-15		s_N / $\binom{N}{2}-3$	s_N / $\binom{N}{2}-1$			
s_N	s_3 / N	s_4 / 2N-2	s_5 / 3N-5	s_6 / 4N-9	s_7 / 5N-14		s_{N-1} / $\binom{N}{2}-2$	s_N / $\binom{N}{2}$			

FIGURE 8.4 - CONSTRUCTION OF AN INV #L FINITE STATE MACHINE SATISFYING $L = \binom{N}{2}$

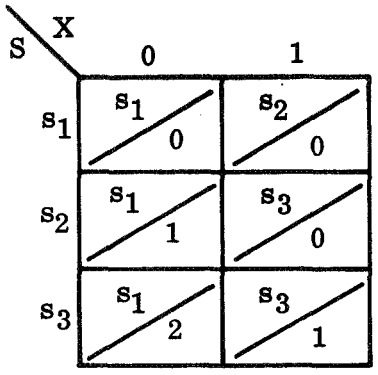


FIGURE 8.5 - A THREE STATE, INV #L FSM WITH L = 3 = $\binom{N}{2}$

Proof: Suppose M is INV #L with $L > N$. Suppose further that there exist s_0, a^L and b^L as defined in the statement of the theorem. Since $L > N$, it follows that both $\delta(s_0, a_1 a_2 \cdots a_i) = \delta(s_0, a_1 a_2 \cdots a_j)$ and $\delta(s_0, b_1 b_2 \cdots b_n) = \delta(s_0, b_1 b_2 \cdots b_m)$ for some $i < j \leq L$ and $n < m \leq L$. But this implies that the output sequence $\lambda(s_0, a_1 a_2 \cdots a_i (a_{i+1} a_{i+2} \cdots a_j)^k)$ coincides with the first $i + (j-i)^k$ letters of the output sequence $\lambda(s_0, b_1 b_2 \cdots b_n (b_{n+1} b_{n+2} \cdots b_m)^t)$ for some arbitrarily large k and for any t such that $n + (m-n)^t \geq i + (j-i)^k$. It follows that M is not INV #L for any L.

In this chapter we have presented several results concerning upper bounds on inverse delay. We remark in conclusion, however, that a satisfactory upper bound on L for the general class of INV #L finite state machines has not been obtained. Such a bound should be based on the size of input and output alphabets as well as on the order of the state set. We remark also that even if attention is limited to binary machines a tight upper bound on L has not as yet been derived. We believe that in the binary case this bound will vary only linearly with the order of the state set.

CHAPTER IX

CONCLUSIONS AND RECOMMENDATIONS FOR CONTINUED RESEARCH

Chapters I through VIII contain many rather diverse results concerning the invertibility of finite state machines and of some special classes of such machines. Although many results are given in these chapters, it is apparent that several important questions remain unanswered. Continued research could be profitable in several of the areas which were considered. This final chapter will summarize the main results which were obtained and point out certain of the more important remaining unsolved problems.

In Chapter I a very general inverse definition was considered. Delay L inverses were defined with respect to a particular state. Necessary and sufficient conditions for the existence of such inverses were given. Certain characteristics of finite state machines which have inverses were shown. An inverse construction procedure applicable to any FSM for which an inverse exists was presented. As a consequence of the construction an upper bound on the number of states in the minimal inverse was derived. The bound appears quite loose, however, and further research should yield an improved upper bound.

A more restricted class of inverses was considered in Chapter II. An FSM is said to have a general delay L inverse if it has a delay L inverse with respect to every state. An FSM is INV #L if L is the least integer such that there exists a general delay L inverse. Finally, a machine is invertible if it

is INV #L for some L. Attention in Chapter II was confined to the class of strongly connected FSM's with common input and output set orders (#X = #Y). The main results of Chapter II are embodied in the derivation of several structural properties of invertible FSM's of the class considered. These properties concern the size of certain final state sets (S_f (s, y^n)) and output sequence sets (Y^n (s)) defined as in Chapter I. A certain uniformity in the order of these sets for invertible machines was demonstrated. Further investigation of the relationships among the cardinalities of these and other sets defined as in Chapter I may yield some interesting results.

Chapter II also presents a necessary and sufficient condition for strongly connected FSM's with #X = #Y to be INV #L. It was shown that such machines are INV #L if and only if for every output sequence y^n and for any n there exists a state in every final state set of the form, S_f (s, y^L), which allows y^n.

The concepts of information losslessness (IL) and information losslessness of finite order as established by Huffman were considered in Chapter III. Relations between these concepts and the notions of invertibility given in Chapters I and II were given. A necessary and sufficient condition for a strongly connected machine with #X = #Y to be IL was shown. This condition is similar to the condition shown to be necessary and sufficient for the INV #L property but is weaker in that it is only required that for any output sequence y^n for any n there exists a state that allows y^n.

Chapter III presents an upper bound on the least integer n such that if an N state FSM is not IL, then there exists a state s_0 and input sequences $a^n \neq b^n$

such that both $\lambda(s_0, a^n) = \lambda(s_0, b^n)$ and $\delta(s_0, a^n) = \delta(s_0, b^n)$. The bound was given as $n \leq \binom{N}{2} + 1$. Chapter III also considers bounds on the greatest integer n such that every output sequence y^n is allowed on an N state, strongly connected, non-IL FSM with #X = #Y. The problem was not solved satisfactorily, however, and the need for further work in the derivation of a good bound is indicated.

A new type of state equivalence, namely, "output equivalence", was presented in Chapter IV. It was shown that state reduction resulting from the deletion of output equivalent states preserves invertibility and in some cases information losslessness. In addition, it was shown that, for a certain class of machines, important structural properties are preserved under state reduction of output equivalent states. In particular, for strongly connected, invertible machines with #X = #Y, the order of the final state set, $\#S_f(s, y^n)$, is invariant under state minimization for any n. It was further shown that, although inverse delay may not be preserved by the reduction of output equivalent states, there exists at least one output minimal version which is INV #L if the original machine is INV #L.

It is considered quite possible that further study of the relationships between IL and invertible finite state machines and their output minimal versions will provide some important results. Moreover, the output equivalence relation itself and the partitions π_n generated by successive application of n - output equivalence relations; $n = 1, 2, 3, \cdots\cdots$; to the state set appear worthy of further study. In particular, an upper bound on the integer n such that $\pi_{n-1} \neq \pi_n$ is considered a worthwhile objective for continued research.

The class of finite input memory μ(FIM (μ)) machines was considered in Chapter V. Several structural properties which pertain specifically to FIM (μ), non-degenerate, maximal state, invertible machines were shown. A uniformity in the number of states which allow any given output sequence of length $n \geq L$ was demonstrated. In addition, it was shown for any n and any length n output sequence y^n, that the same number of distinct pairs of initial states and length n input sequences yield the output sequence y^n.

Several properties of the output function associated with FIM, non-degenerate, invertible machines were considered. Sufficient conditions for an output function to be characteristic of a binary, FIM, non-degenerate, invertible machine were given. Similar conditions were given for IL but not invertible behavior. An important unsolved problem and one which merits continued investigation consists of the extension of these conditions to show both necessity and sufficiency.

In Chapter VI the invertibility of finite output memory μ(FOM (μ)) machines was investigated. A necessary and sufficient condition for a non-degenerate, FOM machine to be information lossless was given. It was concluded that for non-degenerate FOM machines, the IL property implies invertibility. Moreover, the IL property implies an instantaneous inverse. Hence, FOM machines which are INV #L for $L \geq 1$ do not exist.

Chapter VII considered the class of linear sequential circuits (LSC's). A problem related to the existence of a special class of inverse LSC's was

investigated. A necessary and sufficient condition for the existence of feedforward inverses for the general class of LSC's was derived. A procedure for the construction of feedforward inverses, when they exist, results from the constructive proof of sufficiency. In addition, it was shown that the inverse delay resulting from such a construction is minimal over all classes of inverses. The material contained in Chapter VII is basically an extension of a result due to Massey and Sain who derived a similar condition for the class of feedforward LSC's.

The question of upper bounds on L for INV #L machines was considered in Chapter VIII. By restriction to binary machines with maximum final state set order two, it was possible to show that $L \leq N/2$, where N is the order of the state set, is a tight upper bound on inverse delay. It is conjectured that the upper bound on inverse delay for any binary machine grows only linearly with N and that, in general, the bound decreases with increasing final state set order. It was shown in Chapter VIII that the N/2 bound can be achieved with equality for strongly connected, binary machines with maximum final state set orders two and four. No such strongly connected examples were found, for larger final state set orders, however. The derivation of an upper bound on inverse delay which grows only linearly with N for either the general class of binary machines or the class of strongly connected binary machines remains an important unsolved research problem.

It is noted in Chapter VIII that if the orders of input and output alphabets are arbitrary then it is possible to construct machines which are INV #L for

$L = \binom{N}{2}$. Hence, this well known upper bound on L is tight for the general class of finite state machines. It is implied, however, that the maximum inverse delay depends not only on the order of the state set, but on the orders of input and output alphabets as well. It is conjectured that a tight bound on L for the general class of INV #L FSM's will include all three quantities.

In conclusion, one more unsolved problem for continued research is noted. This problem consists of the determination of an upper bound on L for INV #L, FIM (μ) machines. The bound is evidently given by $L \leq \mu$. At present this is only conjecture, however.

APPENDIX A

EXAMPLE OF FEEDFORWARD INVERSE CONSTRUCTION

Consider the four output, three input, binary LSC with transfer function matrix

$$H(D) = \begin{bmatrix} D^2 + D & 1 & 1 \\ 0 & D & 1 \\ D^2 + D & 1 & 1/(D+1) \\ 1 & D+1 & 0 \end{bmatrix}$$

The matrix H (D) has rank three over the field of rational functions over GF (2). It follows that H (D) is invertible. However, the question of feedforward inverse existence is not immediately answered. Inversion of any 3 x 3 submatrix of H (D) does not directly yield an inverse with feedforward realization. In order to test for the existence of such an inverse we make use of Equation (10) of Chapter VII. By direct computation of the elements of Equation (10) we have

$Q(D) = \text{lcm}\left[\text{denominator polynomials of } H(D)\right] = D + 1,$

$\Delta(D) = \gcd\left[\Delta_i(D)\right] = D^2 + 1;\ i = 1, 2, 3, 4,$

$C(D) = \gcd\left[c_{ij}(D)_n\right] = D + 1;\ i = 1, 2, 3;\ j = 1, 2, 3,;\ n = 1, 2, 3, 4,$

and $\gcd\left[\Delta(D), Q(D)\right] = D + 1.$

Evaluation of the left hand side of Equation (10) yields

$$\frac{\Delta(D)}{\gcd\left[\Delta(D), Q(D)\right] C(D)} = \frac{D^L}{\beta(D)} = \frac{D^0}{1}.$$

Therefore, a feedforward inverse does exist. Since L = 0, the inverse delay is zero.

The inverse may be constructed by utilization of Equation (30) of Chapter VII or

$$R'(D)\,\underline{T}(D) = \beta(D)\,Q'(D) \sum_{i=1}^{\binom{N}{K}} B_i(D)\,C'(D)_i\,\underline{T}(D)_i = D^L \underline{I}(D) \quad .$$

Proceeding with the computation of the elements of the above we note that $\beta(D) = 1$ has already been determined. $Q'(D)$ can be found from

$$Q'(D) = Q(D)/\gcd\left[\Delta(D),\ Q(D)\right] = 1 \quad .$$

The four 3 x 3 submatrices of G (D) have determininants given by

$$\Delta_1(D) = D^6 + D^5 + D^4 + D^3 \ ; \qquad \text{rows } 1, 2, 3 \ ,$$

$$\Delta_2(D) = D^6 + D^5 + D^4 + D^2 + D + 1 \ ; \qquad \text{rows } 1, 2, 4 \ ,$$

$$\Delta_3(D) = D^6 + D^3 + D^2 + D \ ; \qquad \text{rows } 1, 3, 4 \ ,$$

$$\Delta_4(D) = D^6 + D^5 + D + 1 \ ; \qquad \text{rows } 2, 3, 4 \ .$$

The row designations given for the $\Delta_i(D)$; $i = 1, 2, 3, 4$; define the rows of $G(D) = H(D)/Q(D)$ used to form $G(D)_i$. A possible set of polynomials $B_i(D)$ which satisfy Equation (23) of Chapter VII is given by

$$B_1(D) = 0 \ ,$$

$$B_2(D) = 0 \ ,$$

$$B_3(D) = D^2 + D + 1 \ ,$$

$$B_4(D) = D^2 + 1 \ .$$

The reduced adjoint matrices $C'(D)_i$ defined by Equation (29) of Chapter VII for i = 3 and i = 4 are given by

$$C'(D)_3 = \begin{bmatrix} D+1 & D^2+1 & D \\ 1 & D+1 & D^3+D^2 \\ D^4+D^3+D^2+1 & D^4+D^3+D^2+1 & 0 \end{bmatrix},$$

$$C'(D)_4 = \begin{bmatrix} D+1 & D^2+1 & 1 \\ 1 & D+1 & D^3+D \\ D^4+D^3+D^2+1 & D^2+D & D^4+D^2 \end{bmatrix}.$$

Note that it is not necessary to compute $C'(D)_1$ and $C'(D)_2$ since $B_1(D) = B_2(D) = 0$. Since $\beta(D) = Q'(D) = 1$, the inverse matrix $R'(D)$ can be obtained by summing the entries in $B_3(D)\,C'(D)_3$ and $B_4(D)\,C'D_4$ which relate particular inputs and outputs. The result of the summation in this case is

$$R'(D) = \begin{bmatrix} D^3+1 & D^3+D^2+D+1 & D^3+D & D^3+D+1 \\ D^2+D+1 & D^2+1 & D^2+D & D^2+D \\ D^6+D^4+D+1 & D^6+D^5+D^3+1 & D^6+D^3+D^2+1 & D^6+D^2 \end{bmatrix}.$$

Since all entries in $R'(D)$ are polynomials, the inverse has a feedforward realization.

REFERENCES

- Martin Cohn, "Controllability in Linear Sequential Networks", IRE Transactions on Circuit Theory, Vol. CT-9, No. 1, March 1962, pp. 74-78.

- Martin Cohn, "Properties of Linear Machines", Journal For The Association of Computing Machinery, Vol. II, No. 3, July 1964, pp. 296-301.

- S. Even, "Tests for Unique Decipherability", IEEE Transactions on Information Theory, Vol. IT-9, April 1963, pp. 109-112.

- S. Even, "On Information Lossless Automata of Finite Order", IEEE Transactions on Electronic Computers, Vol. EC-14, August 1965, pp. 561-569.

- G. D. Forney, "Convolutional Codes I : Algebraic Structure", IEEE Transactions on Information Theory, Vol. IT-16, No. 6, November 1970, to appear.

- A. Gill, Introduction To The Theory of Finite-State Machines, McGraw-Hill, 1962, pp. 123-125, 149-153.

- A. Gill, Linear Sequential Circuits, McGraw-Hill, 1966.

- F. Hennie, Finite-State Models For Logical Machines, John Wiley & Sons, Inc., 1968.

- D. A. Huffman, "Information Conservation and Sequence Transducers", Proceedings Symposium on Information Networks, Polytechnic Institute of Brooklyn, April 12-14, 1954, pp. 291-307.

- D. A. Huffman, "Canonical Forms for Information Lossless Finite-State Logical Machines", Transactions of the IRE Professional Group on Circuit Theory, Vol. CT-6, Special Supplement, May 1959, pp. 41-59.

- J. L. Massey and M. K. Sain, "Inverses of Linear Sequential Circuits", IEEE Transactions on Computers, Vol. C-17, April 1968, pp. 330-337.

- J. L. Massey and M. K. Sain, "Postscript to Inverses of Linear Sequential Circuits", IEEE Transactions on Computers, Vol. C-17, December 1968, p. 1177.

- F. Preparata, "Convolutional Transformations of Binary Sequences : Boolean Functions and Their Resynchronizing Properties", IEEE Transactions on Electronic Computers, Vol. EC-15, December 1966, pp. 898-908.

- K. Vairavan, "On The Memory of Finite State Machines", Technical Report No. EE-683, University of Notre Dame, Department of Electrical Engineering, April 7, 1968.

- L. R. Welch, "Labelled Oriented Graphs which are Onto", N. S. A. Technical Journal, October 1966, pp. 43-49.